PARAMETRIC STANDARD BASIS, DEGREE BOUND AND LOCAL HILBERT-SAMUEL FUNCTION

ROUCHDI BAHLOUL

Abstract. We propose a general study of standard bases of polynomial ideals with parameters in the case where the monomial order is arbitrary. We give an application to the computation of the stratification by the local Hilbert-Samuel function. Moreover, we give an explicit upper bound for the degree of a standard basis for an arbitrary order and also for the number of the possible affine or local Hilbert-Samuel functions depending on the number of variables and the maximal degree of the given generators.

Introduction and statement of the main results

In affine algebraic geometry, several (global) objects can be computed using Gröbner bases such as the affine Hilbert polynomial or free resolutions and parametric Gröbner bases may be seen as a tool for studying these objects under deformations. In the same way, parametric standard bases (with respect to local monomial orders) can be used to study local objects under deformations.

To our knowledge, most of the existing papers on parametric Gröbner or standard bases concern *global* monomial orders (see e.g. Lejeune-Jalabert and Philippe [LePh89], Gianni [Gi89], Weispfenning [We92, We03], Kalkbrenner [Ka97], Montes [Mo02], Sato and Suzuki [SaSu03], Gonzalez-Vega et al. [GTZ05]). In [As94] worked with both global and local orders (to study flatteners of projections) where the ring of the coefficients is polynomial. In [As05], Aschenbrenner made a general study of parametric ideals in power series rings. He also treated the case where the input generators are polynomials (and the monomial order is local). In [Ba06] the author applied parametric standard bases in rings of differential operators to study the local Bernstein-Sato polynomial of a deformation of a hypersurface singularity.

In the present paper, we propose a general study of parametric standard bases for ideals in some ring $\mathcal{C}[x_1, \ldots, x_n]$ where the monomial order on the x-variables is *arbitrary* and the ring $\mathcal{C}$ of parameters is also arbitrary.

We shall be concerned both by existencial and by algorithmic questions. As an application, an algorithm for computing the stratification by the local Hilbert-Samuel function is given. Moreover, as an application of a paper by T. Dubé [Dub90], we give some bounds for the degree of standard bases with respect to any monomial order and also for the number of the possible local or affine Hilbert-Samuel functions.

Before stating the main results, let us introduce some notations.

Throughout the paper, $\mathcal{C}$ shall denote an integral domain. This ring shall be seen as the ring of parameters. Let n be a positive integer and let x denote the set $(x_1, \ldots, x_n)$ of indeterminates.
Let $\preceq$ be a monomial order on the monomials $x^\alpha = \prod_i x_i^{\alpha_i}$ ($\alpha \in \mathbb{N}^n$). We don't suppose $\preceq$ to be a well-ordering (i.e. global).

A **specialization of** $\mathcal{C}$ is a ring homomorphism $\sigma : \mathcal{C} \to \mathbf{K}$ to some field $\mathbf{K}$. A specialization σ of $\mathcal{C}$ induces a ring homomorphism $\mathcal{C}[x] \to \mathbf{K}[x]$ that we shall denote by the same symbol σ.

The next examples illustrate the situations that we shall consider in this paper.

Example 0.0.1. *(1) Let $\mathbf{k} \subset \mathbf{K}$ be two fields and $y = (y_1, \ldots, y_m)$ be a set of indeterminates. For any $y_0 \in \mathbf{K}^m$ the map $(\mathbf{k}[y] \to \mathbf{K}, P \mapsto P(y_0))$ is a specialization of $\mathbf{k}[y]$ to $\mathbf{K}$. It induces the natural map $(\mathbf{k}[x, y] \to \mathbf{K}[x], f \mapsto f_{|y=y_0})$.*

(2) The previous example is a particular case of the following one. Given a prime ideal, that is $\mathcal{P} \in \mathrm{Spec}(\mathbf{K}[y])$, the natural composition map $\sigma_{\mathcal{P}} : \mathbf{k}[y] \to \mathbf{K}[y] \to \mathbf{K}[y]/\mathcal{P} \subset \mathrm{Frac}(\mathbf{K}[y]/\mathcal{P})$ is a specialization. For $y_0 = (y_{0,1}, \ldots, y_{0,m}) \in \mathbf{K}^m$, denote by $m_{y_0} = \sum \mathbf{K}[y](y_j - y_{0,j})$ the maximal ideal associated with y_0. Then $\sigma_{m_{y_0}}$ is identified with the specialization of (1).

(3) Let d be a positive integer. Set $q = \binom{n+d}{n}$. This number is the dimension of the vector space $\oplus_{|\alpha| \leq d} \mathbf{K} x^\alpha$ for any field $\mathbf{K}$. Consider the variables $a = (a_{j,\alpha} | j = 1, \ldots, q; \alpha \in \mathbb{N}^n, |\alpha| \leq d)$. Set $N = q^2$. It is the number of the $a_{j,\alpha}$'s.

For $j = 1, \ldots, q$, set $f_j = \sum_{|\alpha| \leq d} a_{j,\alpha} x^\alpha \in \mathbb{Z}[a, x] = \mathbb{Z}[a][x]$. Let $J = J(n, d)$ denote the ideal of $\mathbb{Z}[a, x]$ generated by $f_1, \ldots, f_q$.

Put $\mathcal{C} = \mathbb{Z}[a]$. Let $\mathbf{K}$ be any field. For $a_0 \in \mathbf{K}^N$ we have the natural map $\sigma_{a_0} : \mathcal{C} \to \mathbf{K}, P(a) \mapsto P(a_0)$. This specialization induces a map $\sigma_{a_0} : \mathbb{Z}[a, x] \to \mathbf{K}[x]$.

This kind of specialization is interesting because for any field $\mathbf{K}$ and for any ideal I of $\mathbf{K}[x]$ generated by polynomials whose degree is at most d, there exists $a_0 \in \mathbf{K}^N$ such that $I = \mathbf{K}[x]\sigma_{a_0}(J)$.

0.1. Main results for parametric standard bases.

For a non-zero polynomial $f \in R[x]$ with coefficients in some ring R, $\exp_{\preceq}(f) \in \mathbb{N}^n$ denotes the leading exponent of f with respect to $\preceq$, it is defined as the maximum of the α's such that x^α appears in the development of f.

Theorem 0.1.1. *Let $J \subset \mathcal{C}[x]$ and $\mathcal{Q} \subset \mathcal{C}$ be finitely generated ideals such that $J \not\subseteq \mathcal{C}[x]\cdot\mathcal{Q}$. There exists a finite set $\mathcal{G} \subset J$ and finitely many $h_i \in \mathcal{C} \smallsetminus \mathcal{Q}$ such that if we set $h = \prod_i h_i$ then for any field $\mathbf{K}$ and any specialization $\sigma : \mathcal{C} \to \mathbf{K}$ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$ the following holds :*

- *$\sigma(\mathcal{G})$ is a $\preceq$-standard basis of $\mathbf{K}[x]\sigma(J)$.*
- *for each $g \in \mathcal{G}$, $\exp_{\preceq}(\sigma(g))$ is independent of σ.*

Notice that the set of the specializations σ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$ may be empty:

Lemma 0.1.2. *Let $\mathcal{Q} \subset \mathcal{C}$ be an ideal and $h \in \mathcal{C}$ then:* (1) $\Longrightarrow$ (2) $\iff$ (3), *where:*

(1) $h \in \sqrt{\mathcal{Q}}$,
(2) *For any field* $\mathbf{K}$ *and any specialization* $\sigma : \mathcal{C} \to \mathbf{K}$ *we have:* $\sigma(\mathcal{Q}) = \{0\} \Rightarrow \sigma(h) = 0$,
(3) $V(\mathcal{Q}) \subset V(h)$ *where* $V(\cdot)$ *means the affine scheme defined by (see the notations 0.4).*

Proof. Assume that $h^i \in \mathcal{Q}$ for some positive integer i. For a specialization $\sigma : \mathcal{C} \to \mathbf{K}$, if $\sigma(\mathcal{Q}) = \{0\}$ then $(\sigma(h))^i = \sigma(h^i) = 0$ wich implies $\sigma(h) = 0$. Thus (1) $\Rightarrow$ (2). Assume (2). Let $\mathcal{P} \subset \mathcal{C}$ be prime such that $\mathcal{Q} \subset \mathcal{P}$. Condition (2) applied to $\sigma_{\mathcal{P}}$ (as defined in Example 0.0.1(2)) implies that $\sigma_{\mathcal{P}}(h) = 0$ which means that $h \in \mathcal{P}$. Thus we have (2) $\Rightarrow$ (3). Conversely assume Condition (3). Let σ be a specialization such that $\sigma(\mathcal{Q}) = \{0\}$. Then $\ker(\sigma) \in V(\mathcal{Q})$. Therefore $\sigma(h) = 0$. $\square$

In 4.3 we shall prove the last implication for $\mathcal{C} = \mathbf{k}[y]$.

Corollary 0.1.3. *Assume that* $\mathcal{C}$ *is noetherian and let* J *be a finitely generated ideal of* $\mathcal{C}[x]$. *There exists a finite set of triples* $(\mathcal{G}_k, \mathcal{Q}_k, h_k)$ *where each* $\mathcal{G}_k \subset J$ *is finite, each* $\mathcal{Q}_k \subset \mathcal{C}$ *is an ideal and each* $h_k \in \mathcal{C}$ *and there exists an ideal* $\mathcal{I} \subset \mathcal{C}$ *such that*

- $\mathrm{Spec}(\mathcal{C}) = (\bigcup_k V(\mathcal{Q}_k) \smallsetminus V(h_k)) \cup V(\mathcal{I})$,
- *for any specialization* σ *of* $\mathcal{C}$, *if* $\sigma(\mathcal{I}) = \{0\}$ *then* $\sigma(J) = \{0\}$,
- *for any* k, *for any field* $\mathbf{K}$ *and any specialization* $\sigma : \mathcal{C} \to \mathbf{K}$ *such that* $\sigma(\mathcal{Q}_k) = \{0\}$ *and* $\sigma(h_k) \neq 0$,
  - $\sigma(J) \neq \{0\}$,
  - $\sigma(\mathcal{G}_k)$ *is a* $\preceq$*-standard basis of* $\mathbf{K}[x]\sigma(J)$,
  - *for each* $g \in \mathcal{G}_k$, $\exp_{\preceq}(\sigma(g))$ *is independent of* σ.

Here again, $V(\cdot)$ stands for the affine scheme (see 0.4).

If we form the union of the obtained $\mathcal{G}_k$ we get a comprehensive $\preceq$-standard basis $\mathcal{G}$ (see [We92, We03, Mo02] in the case of a well-ordering $\preceq$):

Corollary 0.1.4. *Let* $\mathcal{C}$ *be noetherian and let* $J \subset \mathcal{C}[x]$ *be a finitely generated ideal. There exists a finite set* $\mathcal{G} \subset J$ *such that for any specialization* $\sigma : \mathcal{C} \to \mathbf{K}$ *such that* $\sigma(J) \neq \{0\}$, $\sigma(\mathcal{G})$ *is a* $\preceq$*-standard basis of* $\mathbf{K}[x]\sigma(J)$.

Definition 0.1.5. *The ring* $\mathcal{C}$ *is called* ***detachable*** *if for any* $h, h_1, \ldots, h_q \in \mathcal{C}$ *there is a finite algorithm for deciding if* $h \in \sum_{j=1}^{q} \mathcal{C} \cdot h_j$.

Proposition 0.1.6. *Suppose that* $\mathcal{C}$ *is detachable.*

(1) The set $\mathcal{G}$ *and the elements* h_i *of Theorem 0.1.1 can be constructed algorithmically (in a finite number of steps).*
(2) Assume that the intersection of two finitely generated ideals is computable in $\mathcal{C}$ *then the triples* $(\mathcal{G}_k, \mathcal{Q}_k, h_k)$ *and the ideal* $\mathcal{I}$ *of Corollary 0.1.3 can be constructed algorithmically.*
Moreover, if for any specialization $\sigma : \mathcal{C} \to \mathbf{K}$, $\sigma(J) \neq \{0\}$ *then we don't need to assume that the intersection of ideals in* $\mathcal{C}$ *is computable.*

Given a computable field $\mathbf{k}$ and a set of variables $y = (y_1, \ldots, y_m)$, then $\mathbf{k}[y]$ and $\mathbb{Z}[y]$ are both detachable. For $\mathbb{Z}[y]$, see e.g. [Ay83], [GaMi94] and [As04] (and all the citations in [As04]).

0.2. **Constructibility results for Hilbert-Samuel functions.** Let $\mathbf{k} \subset \mathbf{K}$ be two fields where $\mathbf{k}$ is supposed to be computable.

Let I be an ideal in $\mathbf{k}[x]$. The affine Hilbert function associated with I is defined as

$$\mathbb{N} \ni r \mapsto {}^a\mathrm{HF}_{\mathbf{k}[x]/I}(r) = \dim_{\mathbf{k}}(\mathbf{k}[x]_{\leq r}/(I \cap \mathbf{k}[x]_{\leq r}))$$

where $\mathbf{k}[x]_{\leq r}$ is the vector space $\oplus_{|\alpha| \leq r} \mathbf{k} x^\alpha$.

Given $x_0 \in \mathbf{K}^n$, let $\mathbf{K}[[x - x_0]] := \mathbf{K}[[x_1 - x_{0,1}, \ldots, x_n - x_{0,n}]]$ denote the ring of formal power series at x_0. The local Hilbert-Samuel function HSF_{I,x_0} of I at x_0 (over $\mathbf{K}$) is defined by:

$$\mathbb{N} \ni r \mapsto \mathrm{HSF}_{I,x_0}(r) = \dim_{\mathbf{K}}(\mathbf{K}[[x - x_0]]/(\mathbf{K}[[x - x_0]]I + m_{x_0}^r))$$

where m_{x_0} is the maximal ideal of the local ring $\mathbf{K}[[x - x_0]]$.

The notation may seem ambigus if $x_0 \in \mathbf{k}$. In fact for $x_0 \in \mathbf{k} \subset \mathbf{K}$, the local Hilbert-Samuel function of I at x_0 over $\mathbf{k}$ and the one over $\mathbf{K}$ coincide (see Lemma 1.3.2).

There exist numerical polynomials ${}^a\mathrm{HP}_I$ and HSP_{I,x_0} such that for $r \geq r_0$, ${}^a\mathrm{HF}_I(r) = {}^a\mathrm{HP}_I(r)$ and $\mathrm{HSF}_{I,x_0}(r) = \mathrm{HSP}_{I,x_0}(r)$ for some $r_0 \in \mathbb{N}$. These polynomials are called the affine Hilbert polynomial of I and the local Hilbert-Samuel polynomial of I at x_0.

The following is an application of Corollary 0.1.3.

Corollary 0.2.1. *There exists an algorithm for computing a finite partition of $\mathbf{K}^m = \cup W_k$ into constructible sets defined over $\mathbf{k}[x]$ such that for any W_k, the map $W_k \ni x_0 \mapsto \mathrm{HSF}_{I,x_0}$ is constant.*

Let us state another application. Take the notations of Example 0.0.1(3).

Corollary 0.2.2. *Let $J \subset \mathbb{Z}[x, a]$ be the ideal generated by the f_j's. For any field $\mathbf{K}$, there exist a finite partition of $\mathbf{K}^{n+N}$ into constructible subsets W_k with the following properties:*

- *For each stratum W_k, and for any $(a_0, x_0) \in W_k$ the local Hilbert-Samuel function of $J_{|a=a_0} \subset \mathbf{K}[x]$ at $x = x_0$ is constant.*
- *The stratification is defined by ideals in $\mathbb{Z}[a, y]$ that only depend on the integers n and d.*

0.3. **Bounds for Standard bases and Hilbert-Samuel functions.** Applying Corollary 0.1.4 to Example 0.0.1(3), one deduces the existence of a uniform bound $\beta(n, d)$ such that for any field $\mathbf{K}$ and any ideal in $\mathbf{K}[x]$ generated by polynomials in n indeterminates of degree at most d, there is a $\preceq$-standard basis whose elements have degree bounded by $\beta(n, d)$.

In fact, by a direct application of a result by Dubé [Dub90] (see also the recent generalisation [AsLe09]) we obtain an explicit bound from which we deduce a bound for the number of the possible affine or local Hilbert-Samuel functions and polynomials depending on n and d. This answers some questions by Aschenbrenner in the local case (see the discussions after Corollary 3.16 and Lemma 3.18 in [As05]).

Set $D(n, d) = 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$.

Proposition 0.3.1. *Let d and n be positive integers. Let $\preceq$ be any monomial order on the monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Given any field $\mathbf{K}$, let I be an ideal of $\mathbf{K}[x_1, \dots, x_n]$ generated by polynomials of degree at most d. Then there exists a $\preceq$-standard basis of I such that each element has degree at most $D(n, d)$.*

Proposition 0.3.2. *Let d and n be positive integers. There exists a set of functions $\mathcal{HF}(n, d)$ (from $\mathbb{N}$ to $\mathbb{N}$) and a set of numerical polynomials $\mathcal{HP}(n, d)$ that depend only on n and d such that the following holds.*

- *The cardinality of $\mathcal{HP}(n, d)$ is $\binom{nD(n,d)+n}{n}$.*
- *The cardinality of $\mathcal{HF}(n, d)$ is*
$$\binom{nD(n,d)+n}{n} \cdot \prod_{k=0}^{nD(n,d)} \left(1 + \binom{k+n-1}{n-1}\right).$$
- *Let $\mathbf{K}$ be a field. Let $I \subset \mathbf{K}[x_1, \dots, x_n]$ be an ideal generated by polynomials of degree at most d.*
  - ${}^a\mathrm{HP}_{\mathbf{K}[x]/I} \in \mathcal{HP}(n, d)$ *and* ${}^a\mathrm{HF}_{\mathbf{K}[x]/I} \in \mathcal{HF}(n, d)$,
  - *for* $x_0 \in \mathbf{K}^n$, $\mathrm{HSP}_{I,x_0} \in \mathcal{HP}(n, d)$ *and* $\mathrm{HSF}_{I,x_0} \in \mathcal{HF}(n, d)$.

0.4. **Main notations.**

- $\mathbf{k}$: a computable field.
- $\mathbf{K}$: an arbitrary field (In many situations we shall have $\mathbf{k} \subset \mathbf{K}$).
- $\langle f_1, \dots, f_q \rangle$: the ideal generated by the f_i's.
- $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_m)$: sets of variables.
- For $\alpha \in \mathbb{N}^n$ and $\beta \in \mathbb{N}^m$, $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $y^\beta := y_1^{\beta_1} \cdots y_n^{\beta_n}$.
- $\mathcal{C}$: an integral domain (that may be noetherian or/and detachable).
- $\mathrm{Spec}(\mathcal{C}) = \{\mathcal{P} \subset \mathcal{C} \mid \mathcal{P} \text{ is a prime ideal}\}$: the spectrum of $\mathcal{C}$.
- For $S \subset \mathcal{C}$, $V(S) := \{\mathcal{P} \in \mathrm{Spec}(\mathcal{C}) \mid S \subset \mathcal{P}\}$: the affine scheme defined by S.
- σ: a specialization to some field $\mathbf{K}$.
- For an ideal $J \subset \mathbf{k}[x, y]$ and $y_0 \in \mathbf{K}^m$, $J_{|y=y_0} := \mathbf{K}[x] \cdot \{f(x, y_0) \mid f(x, y) \in J\}$: the specialization of J to $y = y_0$.
- For an ideal $I \subset \mathbf{K}[x]$ and $x_0 \in \mathbf{K}$,
  ${}^a\mathrm{HF}_{\mathbf{K}[x]/I}$: the affine Hilbert-function,
  ${}^a\mathrm{HF}_{\mathbf{K}[x]/I}(r) = \dim_{\mathbf{K}} \mathbf{K}[x]_{\le r}/(I \cap \mathbf{K}[x]_{\le r})$;
  HSF_{I,x_0}: the local Hilbert-Samuel function at $x = x_0$,
  $\mathrm{HSF}_{I,x_0}(r) = \dim_{\mathbf{K}}(\mathbf{K}[[x - x_0]]/(m_{x_0}^r + \mathbf{K}[[x - x_0]] \cdot I))$;
  ${}^h\mathrm{HF}_{\mathbf{K}[x]/I}$: the homogeneous Hilbert function (for I homogeneous),
  ${}^h\mathrm{HF}_{\mathbf{K}[x]/I}(r) = \dim_{\mathbf{K}} \mathbf{K}[x]_r/(I \cap \mathbf{K}[x]_r)$

0.5. **Structure of the paper.** In section 1, we recall basic facts about standard bases for polynomial ideals following [GrPf02b] and about Hilbert(-Samuel) functions. In section 2, we prove the results concerning explicit bounds (that is Propositions 0.3.1 and 0.3.2) since their proof is independent of the rest of the paper. In section 3, we introduce the notion of pseudo standard basis modulo some ideal and prove Theorem 0.1.1 and Proposition 0.1.6(1). In 3.2, we shall propose an alternative method in the case

$\mathcal{C} = \mathbf{k}[y]$ using usual standard bases. In section 4, we shall prove Corollary 0.1.3 and Proposition 0.1.6(2). We shall give two algorithm that works with a general ring $\mathcal{C}$ and one for $\mathcal{C} = \mathbf{k}[x]$. In section 5, we shall prove Corollaries 0.2.1 and 0.2.2. We have implemented the algorithm for computing a stratification with constant local Hilbert-Samuel functions in the computer algebra system Risa/Asir [No]. In section 6, we shall present some examples computed with our program[1].

Acknowledgements. This paper began with some discussions with Monique Lejeune-Jalabert and Vincent Cossart to whom I am grateful. I would like to thank Anne Frühbis-Krüger for a reading of a the first version of the manuscript and valuable suggestions.

1. Recalls on standard bases and Hilbert-Samuel functions

For 1.1 and 1.2, the reader can refer to chapters 1 and 2 of the book Singular [GrPf02b].

1.1. **Monomial order and associated ring.** As usual, if $\alpha \in \mathbb{N}^n$ then x^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. A **monomial order** is a total order $\preceq$ on the monomials x^α which is compatible with the product, that is: if $x^\alpha \prec x^{\alpha'}$ then for any α'', $x^{\alpha+\alpha''} \prec x^{\alpha'+\alpha''}$. An order $\preceq$ is called **global** if 1 is the minimal monomial; **local** if 1 is maximal; mixed otherwise. In the sequel, we will identify a monomial order with the induced order on $\mathbb{N}^n$ (which is compatible with the sum).

Let $\mathbf{k}$ be a field. Let A be a ring with inclusions of rings $\mathbf{k}[x] \subseteq A \subseteq \mathbf{k}[[x]]$ and let $\preceq$ be a monomial order. For $f \in A$, write $f = \sum_\alpha c_\alpha x^\alpha$ as a power series expension. We define the support of f as $\mathrm{Supp}(f) = \{\alpha \in \mathbb{N}^n | c_\alpha \neq 0\}$. When they make sense, we define the **leading exponent** of f $\exp(f) = \max_\preceq \mathrm{Supp}(f)$, the **leading term** $\mathrm{lt}_\preceq(f) = x^{\exp_\preceq(f)}$, the **leading coefficient** $\mathrm{lc}_\preceq(f) = c_{\exp_\preceq(f)}$ and the **leading monomial** $\mathrm{lm}_\preceq(f) = \mathrm{lc}_\preceq(f)\mathrm{lt}_\preceq(f)$. These notions always make sense if $A = \mathbf{k}[x]$. If $A = \mathbf{k}[[x]]$, they always make sense if $\preceq$ is local.

Now, let us fix a monomial order $\preceq$. Let $R = \mathbf{k}[x]_\preceq$ be the localization of $\mathbf{k}[x]$ with respect to the multiplicative set $S_\preceq = \{g \in \mathbf{k}[x] \smallsetminus \{0\} | \exp_\preceq(f) = 0\}$. Notice that $R = \mathbf{k}[x]$ if and only if $\preceq$ is global and $R = \mathbf{k}[x]_{(0)}$, that is the localization at 0, if and only if $\preceq$ is local. In any case we have an inclusion of rings $\mathbf{k}[x] \subseteq R \subseteq \mathbf{k}[[x]]$. Thus the notations above apply to the elements of R. Notice that if $f \in R$ and $g \in S_\preceq$ satisfies $gf \in \mathbf{k}[x]$ then $\exp_\preceq(f) = \exp_\preceq(gf)$.

1.2. **Standard bases in the algebraic situation.** For simplification, we shall forget the subscript $\preceq$. For the moment A denotes either $\mathbf{k}[x]$ or $R = \mathbf{k}[x]_\preceq$. Let J be a non zero ideal of A. We define the set of leading exponents $\mathrm{Exp}(J) = \{\exp(f) | f \in J \smallsetminus \{0\}\}$.

Definition 1.2.1. *A finite set $G \subset A$ is called a standard basis of J if $G \subset J$ and $\mathrm{Exp}(J) = \bigcup_{g \in G}(\exp(g) + \mathbb{N}^n)$.*

[1] This program is available on the author's webpage

By Dickson lemma (see [GrPf02b, lemma 1.2.6]), a standard basis exists.

Remark. Assume that $A = \mathbf{k}[x]$. If $\preceq$ is global we shall use the terminology **Gröbner basis** instead of standard basis. A Gröbner basis generates the ideal but a standard basis does not in general.

From now on, $A = R = \mathbf{k}[x]_{\preceq}$.

Definition 1.2.2 ([GrPf02b, Def. 1.6.4])**.** *Let $\mathcal{S}(R)$ denote the set of finite subsets of R. A map* NF $: R \times \mathcal{S}(R) \to R$, $(f, G) \mapsto \mathrm{NF}(f|G)$ *is called a normal form if, for any $f \in R$ and $G \in \mathcal{S}(R)$, we have*

(0) $\mathrm{NF}(0|G) = 0$,
(1) $\mathrm{NF}(f|G) \neq 0 \Rightarrow \exp(\mathrm{NF}(f|G)) \notin \bigcup_{g \in G}(\exp(g) + \mathbb{N}^n)$,
(2) *there exists $u \in R^* = S_{\preceq}$ and for each $g \in G$, there exists $a_g \in R$ such that $r := uf - \mathrm{NF}(f|G)$ has a standard representation: $r = \sum_{g \in G} a_g \cdot g$, with $\exp(r) \succeq \exp(a_g g)$ for all g such that $a_g \neq 0$,*
(3) *if $\{f\} \cup G \subset \mathbf{k}[x]$ then the a_g and u above can be taken in $\mathbf{k}[x]$.*

Remark. This is the definition of a polynomial weak normal form in the terminology of [GrPf02b].

A normal form always exists: see [GrPf02b, 1.6, 1.7] with NFBuchberger when $\preceq$ is global and NFMora in general. NFMora is a variant of Mora's division [Mo82].

Lemma 1.2.3 ([GrPf02b, lemma 1.6.7])**.** *Let J be an ideal of R, G be a standard basis of J and* NF *be a normal form. For any $f \in R$, $f \in J$ if and only if* $\mathrm{NF}(f|G) = 0$.

Consequently, G generates J over R (but not over $\mathbf{k}[x]$ in general).

Definition 1.2.4. *Let f, g be non zero elements in R. Set $\alpha = \exp(f)$, $\beta = \exp(g)$ and $\gamma = (\gamma_1, \dots, \gamma_n)$ with $\gamma_i = \max(\alpha_i, \beta_i)$. We define the S-polynomial (or S-function) of f and g as: $S(f,g) := \mathrm{lc}(g)x^{\gamma-\alpha}f - \mathrm{lc}(f)x^{\gamma-\beta}g$*

Theorem 1.2.5 ([GrPf02b, Th. 1.7.3])**.** *Let $J \subset R$ be an ideal and G a finite subset of J. Let* NF *be a normal form. The following are equivalent:*

(1) *G is a standard basis of J.*
(2) $\mathrm{NF}(f|G) = 0$ *for any $f \in J$.*
(3) *Each $f \in J$ has a standard representation with respect to G that is: there exist some $a_g \in R$ such that $f = \sum_{g \in G} a_g g$ with $\exp(f) \succeq \exp(a_g g)$ for all g such that $a_g \neq 0$.*
(4) *G generates J and for any $g, g' \in G$, $\mathrm{NF}(S(g,g')|G) = 0$.*
(5) *G generates J and for any $g_1, g_2 \in G$, there exist some $a_g \in R$ such that $S(g_1, g_2) = \sum_{g \in G} a_g g$ with $\exp(S(g_1,g_2)) \succeq \exp(a_g g)$ for all g such that $a_g \neq 0$.*

The implications (4) $\Rightarrow$ (1) and (5) $\Rightarrow$ (1) are usually called **Buchberger's criterion**.

Proof. The equivalences (1) $\iff \cdots \iff$ (4) are proven in [GrPf02b]. The implication (3) $\wedge$ (4) $\Rightarrow$ (5) is trivial. Let us show that (5) $\Rightarrow$ (4). Assume by contradiction that for some couple (g_1, g_2), $\mathrm{NF}((g_1,g_2)|G) \neq 0$. Then by Definition 1.2.2(2), $\exp(\mathrm{NF}(S(g_1,g_2)|G)) \notin \cup_{g \in G}(\exp(g) + \mathbb{N}^n)$. This contradicts the standard representation in (5). $\square$

The following remark is a direct consequence of Buchberger's criterion.

Remark 1.2.6. *Let $\mathbf{k}$ and $\mathbf{K}$ be two fields such that $\mathbf{k} \subseteq \mathbf{K}$. Let J be an ideal of $\mathbf{k}[x]_{\preceq}$. If G is a standard basis of J then it is a standard basis of $\mathbf{K}[x]_{\preceq}J$.*

1.3. **Hilbert-Samuel function and Standard basis.** Let us start with a remark.

Remark. *Given an ideal I in $\mathbf{k}[x]$ we defined its local Hilbert-Samuel function at 0 as by $\mathrm{HSF}_{I,0}(r) = \dim_{\mathbf{k}}(\mathbf{k}[[x]]/(\mathbf{k}[[x]]I + \hat{m}^r))$ where $\hat{m}$ denotes the maximal ideal of $\mathbf{k}[[x]]$. In the litterature, one can also find this definition: $\mathrm{HSF}_{I,0}(r) = \dim_{\mathbf{k}}(\mathbf{k}[x]_0/(\mathbf{k}[x]_0 I + m^r))$ where $\mathbf{k}[x]_0$ is the localization of $\mathbf{k}[x]$ at 0 and $m \subset \mathbf{k}[x]_0$ the maximal ideal. These two definitions coincide.*

Proof. Given $r \in \mathbb{N}$, the natural ring homomorphism $\mathbf{k}[x]_0 \to \mathbf{k}[[x]]/(\mathbf{k}[[x]]I + \hat{m}^r)$ is surjective. Its kernal is $(\mathbf{k}[[x]](\mathbf{k}[x]_0 I + m^r)) \cap \mathbf{k}[x]_0$ and it is equal to $\mathbf{k}[x]_0 I + m^r$ by faithfull flateness of $\mathbf{k}[[x]]$ over $\mathbf{k}[x]_0$. $\square$

Given a set $E \subset \mathbb{N}^n$, we define its **Hilbert-Samuel function** $\mathrm{HSF}_E : \mathbb{N} \to \mathbb{N}$ by

$$\mathrm{HSF}_E(r) = \mathrm{card}\{\alpha \in \mathbb{N}^n;\ \alpha \in \mathbb{N}^n \smallsetminus E,\ |\alpha| \leq r\}.$$

A **degree-compatible order** $\preceq$ is a monomial order such that: $|\alpha| < |\alpha'| \Rightarrow x^\alpha \prec x^{\alpha'}$ for any $\alpha, \alpha' \in \mathbb{N}^n$. Such an order is global. A **valuation-compatible order** $\preceq$ is a monomial order such that: $|\alpha| > |\alpha'| \Rightarrow x^\alpha \prec x^{\alpha'}$ for any $\alpha, \alpha' \in \mathbb{N}^n$. Such an order is local.

The following is well-known (see e.g. [CLO92, Chapt. 9, §3, Prop. 4] and [GrPf02b, Prop. 5.5.7]).

Lemma 1.3.1. *Let I be an ideal in $\mathbf{k}[x]$.*

(1) *If $\preceq$ is a degree-compatible order then ${}^a\mathrm{HF}_I = \mathrm{HSF}_{\mathrm{Exp}_{\preceq}(I)}$.*
(2) *If $\preceq$ is a valuation-compatible order then $\mathrm{HSF}_{I,0} = \mathrm{HSF}_{\mathrm{Exp}_{\preceq}(I)}$.*

The next lemma is now trivial (using an affine change of coordinates, Lemma 1.3.1 and Remark 1.2.6).

Lemma 1.3.2. *Let I be an ideal of $\mathbf{k}[x]$ given by generators $f_1, \ldots, f_q$. Let $J \subset \mathbf{k}[x, y]$ be the ideal generated by the $f_i(x+y)$. Let $\mathbf{K}$ be a field containing $\mathbf{k}$. Let $x_0 \in \mathbf{K}^n$ and let $\preceq$ be a valuation-compatible order on the monomials x^α. We have:*

$$\mathrm{HSF}_{I,x_0} = \mathrm{HSF}_{\mathrm{Exp}_{\preceq}(J_{|y=x_0})}.$$

2. Bounds for standard bases and Hilbert-Samuel functions

In this section we shall prove Propositions 0.3.1 and 0.3.2.

2.1. **Bounds for standard bases.** Recall that $\preceq$ is an arbitrary monomial order on the x^α's. Let us add a new variable z and consider the following order $\preceq^z$:

$$x^\alpha z^k \prec^z x^{\alpha'} z^{k'} \iff \begin{cases} |\alpha| + k < |\alpha'| + k' \text{ or} \\ |\alpha| + k = |\alpha'| + k' \text{ and } x^\alpha \prec x^{\alpha'} \end{cases}$$

This order is degree-compatible.

Now we are ready to prove Proposition 0.3.1.

Proof of Proposition 0.3.1. Let $f_1, \dots, f_q$ be polynomials in $\mathbf{K}[x]$ such that the degree of f_j is lower than or equal to d for each j. Set $I = \langle f_1, \dots, f_q \rangle \subset \mathbf{K}[x]$. Writing $f_j = \sum c_{j,\alpha} x^\alpha$, set $h(f_j) = \sum c_{j,\alpha} x^\alpha z^{d_j - |\alpha|}$ where d_j denotes the degree of f_j. The following result by Lazard [La83] is classical (see, e.g., Exerc. 1.7.6 in [GrPf02b]).

Lemma 2.1.1. *Let G be a homogeneous $\preceq^z$-standard basis of the homogeneous ideal $\mathbf{K}[x,z]\{h(f_1), \dots, h(f_q)\}$. Then $G_{|z=1}$ is a $\preceq$-standard basis of I.*

The ideal $I' = \langle h(f_1), \dots, h(f_q) \rangle$ is a homogeneous ideal of $\mathbf{K}[x,z]$ generated by homogeneous polynomials of degree bounded by d. Applying [Dub90, Theorem 8.2] by T. Dubé, one may choose G such that the degree of its elements is bounded by $D(n,d) := 2((d^2/2) + d)^{2^{n-1}}$. Therefore the elements of $G_{|z=1}$ have their degree bounded by $D(n,d)$. □

2.2. **Bounds for affine and local Hilbert-Samuel functions.** Let us begin with a basic combinatorial result.

Lemma 2.2.1. *Let δ be in $\mathbb{N}$. The cardinality of the following set is $\binom{n+\delta}{n}$:*

$$\{(b_1, \dots, b_n) \in \mathbb{N}^n\} |\ b_n \leq b_{n-1} \leq \cdots \leq b_1 \leq \delta\}.$$

Proof. For $(b_1, \dots, b_n)$ in this set one can associate the following monomial: $x_1^{b_1 - b_2} \cdots x_{n-1}^{b_{n-1} - b_n} x_n^{b_n}$. This induces a bijective map from our set to the set of the monomials m of degree $\deg(m) \leq \delta$. It is well-know that the cardinality of the latter is $\binom{n+\delta}{n}$ (see e.g. Lemma 4 page 438 in [CLO92]). □

Here is another technical lemma.

Lemma 2.2.2. *Let J be a monomial ideal in $\mathbf{K}[x_1, \dots, x_n]$. Let G be a finite set of monomials generating J and let $\delta = \max\{\deg(m) | m \in G\}$. Then for any $r \geq n\delta$, ${}^a\mathrm{HF}_{\mathbf{K}[x]/J}(r) = {}^a\mathrm{HP}_{\mathbf{K}[x]/J}(r)$*

Proof. Set $G = \{m_1, \dots, m_q\}$. For $t = (t_1, \dots t_k)$ such that $1 \leq k \leq q$ and $1 \leq t_1 < \cdots < t_k \leq q$. let M_t be the ideal generated by $m_{t_1}, \dots, m_{t_k}$. Finally, for $r \in \mathbb{N}$, set $M_{t,r} = \{x^\alpha; |\alpha| \leq r, x^\alpha \in M_t\}$. Applying the inclusion-exclusion principle, one obtains

$$\begin{aligned} {}^a\mathrm{HF}_{\mathbf{K}[x]/J}(r) &= \binom{r+n}{n} - \mathrm{card}(M_{1,r} \cup \cdots \cup M_{q,r}) \\ &= \binom{r+n}{n} - \sum_{k=1}^{q} (-1)^{k-1} \sum_{1 \leq t_1 < \cdots < t_k \leq q} \mathrm{card}(M_{(t_1, \dots, t_k), r}). \end{aligned}$$

Since $M_{(t_1, \dots, t_k)}$ is generated by $\mathrm{lcm}\{m_{t_1}, \dots, m_{t_k}\}$, we have $\mathrm{card}(M_{(t_1, \dots, t_k), r}) = \binom{r+n-e}{n}$ for every $r \geq e$ where e is the degree of this common multiple. Since $n\delta$ is a bound for the degree of all the common multiples, we conclude that ${}^a\mathrm{HF}_{\mathbf{K}[x]/J}(r)$ is polynomial for $r \geq n\delta$. □

Let us recall some facts from Dubé's paper [Dub90]. For this, we recall that given a homogeneous ideal J in $\mathbf{K}[x_1, \dots, x_n]$ one can define the (homogeneous) Hilbert function

$${}^h\mathrm{HF}_{\mathbf{K}[x]/J}(r) = \dim_{\mathbf{K}}(\mathbf{K}[x]_r / \mathbf{K}[x]_r \cap J)$$

where $\mathbf{K}[x]_r = \oplus_{|\alpha|=r}\mathbf{K}x^\alpha$. Knowing the affine Hilbert function or the homogeneous one is equivalent since we have : ${}^h\mathrm{HF}_{\mathbf{K}[x]/I}(r) = {}^a\mathrm{HF}_{\mathbf{K}[x]/I}(r) - {}^a\mathrm{HF}_{\mathbf{K}[x]/I}(r-1)$ and ${}^a\mathrm{HF}_{\mathbf{K}[x]/I}(r) = \sum_{k=0}^r {}^h\mathrm{HF}_{\mathbf{K}[x]/I}(k)$. Dubé defines the Macaulay constants $(b_0, \ldots, b_n) \in \mathbb{N}^n$ for any homogeneous ideal J. These numbers are uniquely determined and they have some properties :

- $b_0 \geq b_1 \geq \cdots \geq b_n$.
- b_0 is equal to $\min\{b \in \mathbb{N} | \forall r \geq b, {}^h\mathrm{HF}_{\mathbf{K}[x]/J}(r) = {}^h\mathrm{HP}_{\mathbf{K}[x]/J}(r)\}$.
- ${}^h\mathrm{HP}_{\mathbf{K}[x]/I}(r) = \binom{r+n}{n} - 1 - \sum_{k=1}^{n} \binom{r - b_k + k - 1}{k}$.

This shows that the constants $b_1, \ldots, b_n$ uniquely determines and are uniquely determined by the (homogeneous) Hilbert polynomial.

Now let us prove Proposition 0.3.2.

Proof of Prop. 0.3.2. We shall begin by the local case. Recall that we start with an ideal $I \subset \mathbf{K}[x]$ that admits a finite set of generators whose degree is bounded by d. By an affine change of coordinates, we are reduced to the case where $x_0 = 0$. Let us consider a valuation-compatible order.

By Proposition 0.3.1, I admits a standard basis G such that the degree of each element is bounded by $D := D(n, d)$. Let M be the monomial ideal generated by the leading monomials of the g's in G. By Lemma 1.3.1, $\mathrm{HSF}_{\mathbf{K}[x]/I} = {}^a\mathrm{HF}_{\mathbf{K}[x]/M}$. By Lemma 2.2.2, for $r \geq nD$, ${}^a\mathrm{HF}_{\mathbf{K}[x]/M}(r) = {}^a\mathrm{HP}_{\mathbf{K}[x]/M}(r)$.

Using the recalls of Dubé's results, we have that ${}^h\mathrm{HF}_{\mathbf{K}[x]/M}$ and then ${}^a\mathrm{HF}_{\mathbf{K}[x]/M}$ is uniquely determined by some tuple $(b_1, \ldots, b_n)$ such that $nD \geq b_1 \geq \cdots \geq b_n$. By Lemma 2.2.1, the number of these tuples is $\binom{n+nD}{n}$. This proves the part concerning the local Hilbert-Samuel polynomial. Now again by Dubé's results, $b_0 = \min\{b \in \mathbb{N} | \forall r \geq b, {}^a\mathrm{HF}_{\mathbf{K}[x]/M}(r) = {}^a\mathrm{HP}_{\mathbf{K}[x]/M}(r)\}$.

Since $b_0 \leq nD$, ${}^a\mathrm{HF}_{\mathbf{K}[x]/M}(r)$ is determined for all $r \geq nD$. It remains to count the number of possible values that may be taken by ${}^a\mathrm{HF}_{\mathbf{K}[x]/M}(r)$ for $0 \leq r < nD$. For a given $0 \leq r < nD$, ${}^a\mathrm{HF}_{\mathbf{K}[x]/M}(r)$ may be in $\{0, \ldots, \binom{r+n-1}{n-1}\}$. Therefore it may take $\binom{r+n-1}{n-1} + 1$ possible values. Taking the product for all $0 \leq r < nD$ we obtain the bound for the number of the possible local Hilbert-Samuel functions.

Now, the proof concerning the affine Hilbert function and polynomial is the same providing the use of a degree-compatible order instead of a valuation-compatible one. □

3. Parametric standard bases

In this section we shall be concerned by the proof of Theorem 0.1.1 and Proposition 0.1.6(1). In 3.1 we shall treat the case of a general $\mathcal{C}$ and in 3.2 we shall propose another method when $\mathcal{C} = \mathbf{k}[y]$.

3.1. **General case: an analogue of pseudo standard bases.** Recall that $\mathcal{C}$ is an integral domain and $\preceq$ is a monomial order on the x^α's. For $f \in \mathcal{C}[x] \smallsetminus \{0\}$, we can define its leading exponent $\exp_\preceq(f) \in \mathbb{N}^n$, its leading term $\mathrm{lt}_\preceq(f) = x^{\exp_\preceq(f)}$, its leading coefficient $\mathrm{lc}_\preceq(f) \in \mathcal{C}$ and leading monomial

$\mathrm{lm}_{\preceq}(f) = \mathrm{lc}_{\preceq}(f) \cdot \mathrm{lt}_{\preceq}(f)$. In the sequel we shall forget the subscript $\preceq$ and write $\exp(f)$ for $\exp_{\preceq}(f)$.

Set $S_{\preceq} = \{f \in \mathcal{C}[x] | \exp(f) = 0 \text{ and } \mathrm{lc}(f) = 1\}$ then define $R = S_{\preceq}^{-1}\mathcal{C}[x]$ as the localization w.r.t. $S_{\preceq}$.

Definition 3.1.1 (See [GrPf02a] or [GrPf02b, pages 124-125])**.**

- *As in Def. 1.2.2,* $\mathrm{S}(R)$ *denotes the set of finite subsets of* R*. A map* $\mathrm{NF} : R \times \mathcal{S}(R) \to R$, $(f, G) \mapsto \mathrm{NF}(f|G)$ *is called a pseudo normal form if, for any* $f \in R$ *and* $G \in \mathcal{S}(R)$*, we have*
  (0) $\mathrm{NF}(0|G) = 0$
  (1) $\mathrm{NF}(f|G) \neq 0 \Rightarrow \exp(\mathrm{NF}(f|G)) \notin \bigcup_{g \in G}(\exp(g) + \mathbb{N}^n)$
  (2) *There exists* $u \in R$ *such that* $\mathrm{lm}(u)$ *is of the form* $\mathrm{lm}(u) = \prod_{g \in G} \mathrm{lc}(g)^{d_g} \cdot x^0$ *with* $d_g \in \mathbb{N}$*, and for each* $g \in G$*, there exists* $a_g \in R$ *such that* $r := uf - \mathrm{NF}(f|G)$ *has a standard representation:* $r = \sum_{g \in G} a_g \cdot g$*, with* $\exp(r) \succeq \exp(a_g g)$ *for all* g *such that* $a_g \neq 0$.
  (3) *If* $\{f\} \cup G \subset \mathbf{k}[x]$ *then the* a_g *and* u *above can be taken in* $\mathcal{C}[x]$.
- *Given a non-zero ideal* $J \subset R$*, a pseudo standard basis is a finite set* $G \subset J$ *satisfying* $\mathrm{Exp}(J) = \bigcup_{g \in \mathcal{G}}(\exp(g) + \mathbb{N}^n)$.

Notice that our definition of a pseudo standard basis is slightly different to the one given in [GrPf02b, GrPf02a].

Pseudo normal forms exist (NFMora in [GrPf02b] is one) and pseudo standard bases also (by Dickson lemma).

Now let us generalize these constructions. In the sequel $\mathcal{Q} \subset \mathcal{C}$ is a given ideal, not necessarily prime. Given $f \in R = \mathcal{C}[x]_{\preceq}$, we define $\exp^{\mathrm{mod}\mathcal{Q}}(f) := \exp(f \mathrm{mod} \mathcal{Q})$, where $f \mathrm{mod} \mathcal{Q}$ means the class of f in $\mathcal{C}/\mathcal{Q}[x]_{\preceq}$ viewed in $(\mathcal{C}/\mathcal{Q})[[x]]$. We define $\mathrm{lt}^{\mathrm{mod}\mathcal{Q}}(f) := x^{\exp^{\mathrm{mod}\mathcal{Q}}(f)}$. Then $\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(f)$ denotes the coefficient (in $\mathcal{C}$) of $\mathrm{lt}^{\mathrm{mod}\mathcal{Q}}(f)$ in the expension of f, finally $\mathrm{lm}^{\mathrm{mod}\mathcal{Q}}(f) := \mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(f)\mathrm{lt}^{\mathrm{mod}\mathcal{Q}}(f)$.

Now for an ideal $J \subset R$ such that $J \nsubseteq R\mathcal{Q}$, we define $\mathrm{Exp}^{\mathrm{mod}\mathcal{Q}}(J) = \{\exp^{\mathrm{mod}\mathcal{Q}}(f) | f \in J \smallsetminus R\mathcal{Q}\}$.

Definition 3.1.2. *A pseudo standard basis of* J *modulo* $\mathcal{Q}$ *is a finite set* $\mathcal{G} \subset J$ *such that* $\mathrm{Exp}^{\mathrm{mod}\mathcal{Q}}(J) = \bigcup_{g \in \mathcal{G}}(\exp^{\mathrm{mod}\mathcal{Q}}(g) + \mathbb{N}^n)$.

Remark. *Such a set exists by Dickson lemma again. Notice that if* $\mathcal{Q} = (0)$*, we recover the notion of a pseudo standard basis.*

Definition 3.1.3. *A pseudo normal form* $\mathrm{NF}(\cdot|_{\mathcal{Q}}\cdot)$ *modulo* $\mathcal{Q}$ *is a map* $\mathrm{NF}(\cdot|_{\mathcal{Q}}\cdot) : R \times \mathcal{S}(R) \to R$, $(f, G) \mapsto \mathrm{NF}(f|_{\mathcal{Q}}G)$ *such that for any* $f \in R$ *and* $G \in \mathcal{S}(R)$*, we have*

(0) $\mathrm{NF}(q|_{\mathcal{Q}}G) \in R\mathcal{Q}$ *for all* $q \in R\mathcal{Q}$
(1) $\mathrm{NF}(f|_{\mathcal{Q}}G) \notin R\mathcal{Q} \Rightarrow \exp^{\mathrm{mod}\mathcal{Q}}(\mathrm{NF}(f|_{\mathcal{Q}}G)) \notin \bigcup_{g \in G}(\exp^{\mathrm{mod}\mathcal{Q}}(g) + \mathbb{N}^n)$
(2) *There exist some* $a_g \in R$, $q \in R\mathcal{Q}$*, and* $u \in R$ *such that* $\mathrm{lm}^{\mathrm{mod}\mathcal{Q}}(u) = \prod_{g \in G}(\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g))^{d_g} \cdot x^0$ *with* $d_g \in \mathbb{N}$ *and*
$$r := uf - \mathrm{NF}(f|_{\mathcal{Q}}G) = \sum_{g \in G} a_g g + q$$
with $\exp^{\mathrm{mod}\mathcal{Q}}(r) \succeq \exp^{\mathrm{mod}\mathcal{Q}}(a_g g)$ *for all* g *such that* $a_g \neq 0$.
(3) *If* $\{f\} \cup G \subset \mathcal{C}[x]$ *then the* a_g *and* u *and* q *above can be taken in* $\mathcal{C}[x]$.

We define the S-function modulo $\mathcal{Q}$:

Definition 3.1.4. *Let $f, g \in R \smallsetminus R\mathcal{Q}$. Set $\alpha = \exp^{\mathrm{mod}\mathcal{Q}}(f)$, $\beta = \exp^{\mathrm{mod}\mathcal{Q}}(g)$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ with $\gamma_i = \max(\alpha_i, \beta_i)$. We define the S-polynomial (or S-function) of f and g modulo $\mathcal{Q}$ as: $S^{\mathrm{mod}\mathcal{Q}}(f,g) := \mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)x^{\gamma-\alpha}f - \mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(f)x^{\gamma-\beta}g$*

As for standard bases, we have a characterization of pseudo standard bases in terms of pseudo normal forms and S-polynomials.

Proposition 3.1.5. *Let $J \subset R$ be an ideal and G a finite subset of J. Let $\mathrm{NF}(\cdot|_{\mathcal{Q}}\cdot)$ be a pseudo normal form modulo $\mathcal{Q}$. The following are equivalent:*

1. *G is a pseudo standard basis of J modulo $\mathcal{Q}$.*
2. *$\mathrm{NF}(f|_{\mathcal{Q}}G) \in R\mathcal{Q}$ for any $f \in J$.*
3. *For any $f \in J$, there exists $a_g \in R$ for all $g \in G$, $q \in R\mathcal{Q}$, and $u \in R$ with $\mathrm{lm}^{\mathrm{mod}\mathcal{Q}}(u)$ being a product of $\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)$ ($g \in G$) such that: $uf = \sum_{g\in G} a_g g + q$ with $\exp^{\mathrm{mod}\mathcal{Q}}(f) \succeq \exp^{\mathrm{mod}\mathcal{Q}}(a_g g)$ for all g such that $a_g \neq 0$.*
4. *For any $f \in J$, there exists u as above such that $uf \in RG + R\mathcal{Q}$ and for any $g, g' \in G$, $\mathrm{NF}(S^{\mathrm{mod}\mathcal{Q}}(g,g')|_{\mathcal{Q}}G) \in R\mathcal{Q}$.*

Proof. Let us prove (1) $\Rightarrow$ (2). Assume (1) and by contradiction let $f \in J$ be such that $\mathrm{NF}(f|_{\mathcal{Q}}G) \notin R\mathcal{Q}$. Then by Definition 3.1.3(1), $\exp^{\mathrm{mod}\mathcal{Q}}(\mathrm{NF}(f|_{\mathcal{Q}}G)) \notin \bigcup_{g\in G}(\exp^{\mathrm{mod}\mathcal{Q}}(g)+\mathbb{N}^n)$. By Definition 3.1.3(2), $\mathrm{NF}(f|_{\mathcal{Q}}G) \in J + R\mathcal{Q}$ therefore $\exp^{\mathrm{mod}\mathcal{Q}}(\mathrm{NF}(f|_{\mathcal{Q}}G)) \in \mathrm{Exp}^{\mathrm{mod}\mathcal{Q}}(J)$. But this contradicts (1). The proof of (2) $\Rightarrow$ (3) $\Rightarrow$ (1) is a direct application of the definitions. Moreover (3) implies the first part of (4) and (2) implies the second one. It remains to prove (for example) (4) $\Rightarrow$ (1). For this, let us introduce some extra notations. For $f \in R$ let us denote by $(f)_{\mathcal{Q}}$ its image by the natural map $\mathcal{C}[x]_{\preceq} \to \mathcal{C}/\mathcal{Q}[x]_{\preceq} \to \mathrm{Frac}(\mathcal{C}/\mathcal{Q})[x]_{\preceq}$. Let us denote by $(J)_{\mathcal{Q}}$ the ideal generated by $\{(f)_{\mathcal{Q}} |\ f \in J\}$.

Now, let us assume (4) and by contradiction suppose that (1) is not true. There exists $f \in J \smallsetminus R\mathcal{Q}$ such that $\exp^{\mathrm{mod}\mathcal{Q}}(f) \notin \cup_{g\in G}(\exp^{\mathrm{mod}\mathcal{Q}}(g) + \mathbb{N}^n)$. This implies that $\exp((f)_{\mathcal{Q}}) \notin \cup_{g\in G}(\exp(g)_{\mathcal{Q}} + \mathbb{N}^n)$. Hence $(G)_{\mathcal{Q}}$ is not a standard basis of $(J)_{\mathcal{Q}}$.

The first part of (4) implies that $(G)_{\mathcal{Q}}$ generates $(J)_{\mathcal{Q}}$. The second part of (4) combined with Definition 3.1.3(2) implies that for all $g, g' \in G$,

$$S((g)_{\mathcal{Q}}, (g')_{\mathcal{Q}}) = (S^{\mathrm{mod}\mathcal{Q}}(g,g'))_{\mathcal{Q}} = \sum_g (a_g)_{\mathcal{Q}} \cdot (g)_{\mathcal{Q}}$$

with $\exp(S((g)_{\mathcal{Q}}, (g')_{\mathcal{Q}})) \succeq \exp((a_g)_{\mathcal{Q}} \cdot (g)_{\mathcal{Q}})$, hence by Theorem 1.2.5(5), $(G)_{\mathcal{Q}}$ is a standard basis of $(J)_{\mathcal{Q}}$. Contradiction. $\square$

Given $f \in \mathcal{C}[x]$, we define the écart modulo $\mathcal{Q}$: $\text{écart}^{\mathrm{mod}\mathcal{Q}}(f) := \text{écart}(f\mathrm{mod}\mathcal{Q}) = \deg(f\mathrm{mod}\mathcal{Q}) - \deg \mathrm{lt}(f\mathrm{mod}\mathcal{Q})$.

Algorithm 3.1.6 (NFMora $^{\mathrm{mod}\,\bullet}(\bullet|\bullet)$).
Input: $f \in \mathcal{C}[x]$, $G \subset \mathcal{C}[x]$: a finite set, $\mathcal{Q} \subset \mathcal{C}$: an ideal.
Output: $h = \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}}(f|G) \in \mathcal{C}[x]$ a pseudo normal form of f w.r.t. G modulo $\mathcal{Q}$.

• $h := f$;
• $T := G$;
• While ($h \notin \mathcal{C}[x]\mathcal{Q}$ and $T_h := \{g \in T$ such that $\mathrm{lt}^{\mathrm{mod}\mathcal{Q}}(g)|\mathrm{lt}^{\mathrm{mod}\mathcal{Q}}(h)\} \neq \emptyset$)
    • Choose $g \in T_h$ with $\text{écart}^{\mathrm{mod}\mathcal{Q}}(g)$ minimal;
    • If ($\text{écart}^{\mathrm{mod}\mathcal{Q}}(g) > \text{écart}^{\mathrm{mod}\mathcal{Q}}(h)$) then $T := T \cup \{h\}$;
    • $h := S^{\mathrm{mod}\mathcal{Q}}(h, g)$;
• Return h.

All the definitions were made in order to have the following equality: $\mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}}(f|G)\mathrm{mod}\mathcal{Q} = \mathrm{NFMora}(f\mathrm{mod}\mathcal{Q}|G\mathrm{mod}\mathcal{Q})$. This proves both termination and correctness of this algorithm. Moreover this equality proves that $\mathrm{NFMora}^{\ \mathrm{mod}\ \mathcal{Q}}(\bullet|\bullet)$ is pseudo normal form modulo $\mathcal{Q}$.

To be complete, let us give a generalisation of the algorithm "Standard" (see Algorithm 1.7.1 in [GrPf02b]).

Algorithm 3.1.7 (Standard $^{\mathrm{mod}\ \bullet}(\bullet, \bullet)$).
Input: $G \subset R$: a finite set, $\mathcal{Q} \subset \mathcal{C}$: an ideal, NF: a pseudo normal form modulo $\mathcal{Q}$.
Output: $S := \mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NF})$ a pseudo standard basis of the ideal RG modulo $\mathcal{Q}$.
• $S := G$;
• $P := \{(f, g)|f, g \in S, f \neq g\}$;
• While $P \neq \emptyset$
    • Choose $(f, g) \in P$;
    • $P := P \setminus \{(f, g)\}$;
    • $h := \mathrm{NF}(S^{\mathrm{mod}\mathcal{Q}}(f, g)|_{\mathcal{Q}}S)$;
    • If ($h \notin R\mathcal{Q}$) then ($P := P \cup \{(h, f)|f \in S\}$; $S := S \cup \{h\}$);
• Return S.

Claim 3.1.8. *Let G be a finite system of generators of J. The set $\mathcal{G} = \mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}})$ is a pseudo standard basis of J modulo $\mathcal{Q}$.*

Proof. First, notice that $\mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}})$ terminates because, $\mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}})\mathrm{mod}\mathcal{Q} = \mathrm{Standard}(G\mathrm{mod}\mathcal{Q}, \mathrm{NFMora})$. Now let us prove the proposition. The algorithm $\mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}$ terminates when the set P of pairs is empty. This set becomes empty when $\mathrm{NF}(S^{\mathrm{mod}\mathcal{Q}}(f, g)|_{\mathcal{Q}}S)$ is in $R\mathcal{Q}$ for all $(f, g) \in P$. Thus the output $\mathcal{G}$ satisfies Condition (4) of Proposition 3.1.5. Thus, $\mathcal{G}$ is a pseudo standard basis of J modulo $\mathcal{Q}$. $\square$

Proposition 3.1.9.
(1) *Let $\mathcal{G}$ be a pseudo standard basis of J modulo $\mathcal{Q}$ and let $h = \prod_{g \in \mathcal{G}} \mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)$. For any field $\mathbf{K}$ and any specialization $\sigma : \mathcal{C} \to \mathbf{K}$ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$:*
    • *$\sigma(\mathcal{G})$ is a $\preceq$-standard basis of $\mathbf{K}[x]\sigma(J)$.*
    • *for each $g \in \mathcal{G}$, $\exp(\sigma(g)) = \exp^{\mathrm{mod}\mathcal{Q}}(g)$.*
(2) *Moreover if J is generated by a set $G \subset \mathcal{C}[x]$ then it is possible to construct $\mathcal{G}$ inside $\mathcal{C}[x]G$.*

Proving this proposition proves Theorem 0.1.1

Proof. (1) Recall that J is an ideal of $\mathcal{C}[x]$ generated by a given finite set G, and $\mathcal{Q} \subset \mathcal{C}$ is an ideal such that $J \nsubseteq \mathcal{C}[x]\mathcal{Q}$. Fix a field $\mathbf{K}$.

Let $\mathcal{G}$ be a pseudo standard basis of J modulo $\mathcal{Q}$. Let $h \in \mathcal{C}$ be the product of the $\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)$ with $g \in \mathcal{G}$. Let Σ be the set of the specializations $\sigma : \mathcal{C} \to \mathbf{K}$ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$. For $\sigma \in \Sigma$ and for any $g \in \mathcal{G}$, $\sigma(\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)) \neq 0$ and $\exp^{\mathrm{mod}\mathcal{Q}}(g) = \exp(\sigma(g))$ which proves the constancy of $\exp(\sigma(g))$ over $\sigma \in \Sigma$.

Take $\sigma \in \Sigma$. Following $\mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}}$ and NFMora step by step, we obtain that $\sigma(\mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}}(S^{\mathrm{mod}\mathcal{Q}}(g,g')|\mathcal{G}))$ is equal to $\mathrm{NFMora}(S(\sigma(g),\sigma(g'))|\sigma(\mathcal{G}))$ and it is 0 for all $g, g' \in \mathcal{G}$ by Prop. 3.1.5(4).

Proposition 3.1.5(4) implies that $\sigma(\mathcal{G})$ generates $\mathbf{K}[x]\sigma(J)$. Thus Buchberger's criterion (Theorem 1.2.5) implies that $\sigma(\mathcal{G})$ is a standard basis of $\mathbf{K}[x]\sigma(J)$.

(2) By definition $S^{\mathrm{mod}\mathcal{Q}}(f,g) \in \mathcal{C}[x]f + \mathcal{C}[x]g$. Moreover, a pseudo normal form modulo $\mathcal{Q}$ $\mathrm{NF}(\cdot|_{\mathcal{Q}}\cdot)$ (see Condition (4) in Definition 3.1.3) outputs an element that is a combination over $\mathcal{C}[x]$ of the inputs (it is obviously true for $\mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}}$). Finally, in the algorithm $\mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}$, if the inputs are in $\mathcal{C}[x]$ then so are the outputs. □

In order to conclude this part, it remains to prove Proposition 0.1.6(1).

Proof of Prop. 0.1.6(1). Suppose that $\mathcal{C}$ is detachable. Then it is clear that all the "objects" modulo $\mathcal{Q}$ can be computed (such as $\exp^{\mathrm{mod}\mathcal{Q}}(f)$, $S^{\mathrm{mod}\mathcal{Q}}(f,g)$). Thus, given $G \subset \mathcal{C}[x]$, the set $\mathcal{G} = \mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}})$ can be computed in a finite number of steps. □

Remark 3.1.10. Suppose that $\mathcal{C} = \mathbf{k}[y]$ with a computable field $\mathbf{k}$.

From an algorithmic point of view all the "objects" $\mathrm{mod}\mathcal{Q}$ (such as $\exp^{\mathrm{mod}\mathcal{Q}}$) can be computed in the following way. We consider a monomial order on the y^β, say $\leq_0$ and compute a standard or Gröbner basis of $\mathcal{Q}$, say G_0. Then we consider a monomial order, say $\leq$, on the monomials $x^\alpha y^\beta$ whose restriction to y^β is $\leq_0$ (for example the block order $(\preceq, \leq_0)$). Then e.g. by Buchberger's criterion, G_0 is a standard basis of $\mathbf{k}[x,y]\mathcal{Q}$ w.r.t. $\leq$. Given $f \in \mathbf{k}[x,y]$, we compute a normal form $r = \mathrm{NF}_{\leq}(f|G_0)$ and we get $\exp_{\preceq}^{\mathrm{mod}\mathcal{Q}}(f) = \exp_{\preceq}(r)$.

Summing up the results above we get the following algorithm (when $\mathcal{C}$ is detachable).

Algorithm 3.1.11 (PSBmod)**.**
Input: $G \subset \mathcal{C}[x]$: a finite set, $\mathcal{Q} \subset \mathcal{C}$: an ideal.
Output: $\mathrm{PSBmod}(G, \mathcal{Q}) = (\mathcal{G}, H)$ where $\mathcal{G}$ is a pseudo standard basis of $\langle G \rangle$ modulo $\mathcal{Q}$, $H \subset \mathcal{C} \smallsetminus \mathcal{Q}$ is a finite set.
- $H := \emptyset$; $\mathcal{G} := \emptyset$;
- if $G \subset \mathcal{C}[x]\mathcal{Q}$ then Return $(\mathcal{G}, H)$;
- $\mathcal{G} := \mathrm{Standard}^{\mathrm{mod}\mathcal{Q}}(G, \mathrm{NFMora}^{\mathrm{mod}\mathcal{Q}})$;
- for $g \in \mathcal{G}$ do $(H := H \cup \{\mathrm{lc}^{\mathrm{mod}\mathcal{Q}}(g)\})$;
- Return $(\mathcal{G}, H)$.

If $G \subset \mathcal{C}[x]\mathcal{Q}$ then the output is $(\emptyset, \emptyset)$, otherwise we get $(\mathcal{G}, H)$ and setting h as the product of the elements of H, we have that $\mathcal{G}$ specializes to a standard basis for all $\sigma : \mathcal{C} \to \mathbf{K}$ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$.

3.2. **The case $\mathcal{C} = \mathbf{k}[y]$: with standard bases.** In this paragraph, we give an alternative method for computing pseudo standard bases modulo some $\mathcal{Q}$ in the particular case where $\mathcal{C} = \mathbf{k}[y]$.

Denote by $\tilde{J} = J + \mathbf{k}[x,y]\mathcal{Q}$. Let $\leq_0$ be a monomial order on the y^β. For simplicity, we assume that $\leq_0$ is *global*. (In fact, things work even if $\leq_0$ is not global: the proof of Proposition 3.2.2 would need a slight modification.)

Define a block order on $x^\alpha y^\beta$ as $\leq = (\preceq, \leq_0)$, here $\preceq$ is the monomial order on x^α used from the beginning.

Note. For an element $f \in \mathbf{k}[x,y]$, we will work with two types of leading exponents (and of leading terms, coefficients, etc): $\exp_\preceq(f) \in \mathbb{N}^n$ and $\exp_\leq(f) \in \mathbb{N}^{n+m}$.

Remark 3.2.1. *For any $f \in \mathbf{k}[x,y]$, $\exp_\leq(f) = (\exp_\preceq(f), \exp_{\leq_0}(\mathrm{lc}_\preceq(f)))$.*

Let G be a standard basis of $\tilde{J} = J + \mathbf{k}[x,y] \cdot \mathcal{Q}$ w.r.t. $\leq$.

Proposition 3.2.2. *The set $\tilde{\mathcal{G}} = G \smallsetminus \mathbf{k}[x,y] \cdot \mathcal{Q}$ is a $\preceq$-pseudo standard basis of $\tilde{J}$ modulo $\mathcal{Q}$.*

Proof. Take $f \in \tilde{J}$ such that $f \notin \mathbf{k}[x,y]\mathcal{Q}$. We are going to prove that $\exp_\preceq^{\mathrm{mod}\mathcal{Q}}(f) \in \exp_\preceq^{\mathrm{mod}\mathcal{Q}}(g) + \mathbb{N}^n$ for some $g \in G \smallsetminus \mathbf{k}[x,y]\mathcal{Q}$. Since $\mathcal{Q} \subset \tilde{J}$, we may assume $\mathrm{lc}_\preceq^{\mathrm{mod}\mathcal{Q}}(f) = \mathrm{lc}_\preceq(f)$.

Let $c \in \mathbf{k}[y]$ be a normal form of $\mathrm{lc}_\preceq(f)$ with respect to a $\leq_0$-Gröbner basis of $\mathcal{Q}$. Since $\mathrm{lc}_\preceq(f) - c$ is in $\mathcal{Q} \subset \tilde{J}$, we may assume that

$$(\star) \qquad \exp_{\leq_0}(\mathrm{lc}_\preceq(f)) \notin \mathrm{Exp}_{\leq_0}(\mathcal{Q}).$$

By definition of G, there exists $g \in G$ such that $\exp_\leq(f) \in \exp_\leq(g) + \mathbb{N}^{n+m}$. By Remark 3.2.1, this implies $\exp_{\leq_0}(\mathrm{lc}_\preceq(f)) \in \exp_{\leq_0}(\mathrm{lc}_\preceq(g)) + \mathbb{N}^m$. Relation $(\star)$ implies $\mathrm{lc}_\preceq(g) \notin \mathcal{Q}$, i.e. $\mathrm{lc}_\preceq(g) = \mathrm{lc}_\preceq^{\mathrm{mod}\mathcal{Q}}(g)$. Therefore $g \notin \mathbf{k}[x,y]\mathcal{Q}$. By Remark 3.2.1 again, we have $\exp_\preceq(f) \in \exp_\preceq^{\mathrm{mod}\mathcal{Q}}(g) + \mathbb{N}^n$. $\square$

Now let us define $\mathcal{G} \subset J$ as follows. For each element $\tilde{g} \in \tilde{\mathcal{G}}$ let $g \in J$ be such that $g - \tilde{g} \in \mathbf{k}[x,y] \cdot \mathcal{Q}$. We define $\mathcal{G}$ as the set of these g for $\tilde{g} \in \tilde{\mathcal{G}}$. The set $\mathcal{G}$ is not uniquely determined of course.

As a trivial consequence of the definition of $\tilde{J}$ we obtain:

Corollary 3.2.3. *$\mathcal{G}$ is a $\preceq$-pseudo standard basis of J modulo $\mathcal{Q}$.*

Hence, this ends the second proof of Theorem 0.1.1.

Now in order to end this part, we have to propose an algorithmic construction for such a $\mathcal{G}$. We think that the smplest way is to construct in parallel the sets $\tilde{\mathcal{G}}$ and $\mathcal{G}$. For this, we propose a modification of the algorithm Standard.

Algorithm 3.2.4 (ModifiedStandard($\bullet, \bullet, \bullet$))**.**
Input: $G_1, G_2 \subset \mathbf{k}[x,y]$: finite sets, NF: a normal form.
Output: $S :=$ ModifiedStandard(G_1, G_2, NF) where $S = \{(\tilde{g}_1, g_1), \ldots, (\tilde{g}_s, g_s)\}$ is a finite set such that $\{\tilde{g}_1, \ldots, \tilde{g}_s\}$ is a standard basis of $\langle G_1 \cup G_2 \rangle$ and for all i, $g_i \in \langle G_1 \rangle$ and $\tilde{g}_i - g_i \in \langle G_2 \rangle$.
- $S := \bigcup_{g \in G_1} \{(g,g)\} \cup \bigcup_{g \in G_2} \{(g,0)\}$;
- $P := \{((\tilde{f}, f), (\tilde{g}, g)) |\ (\tilde{f}, f), (\tilde{g}, g) \in S, \tilde{f} \neq \tilde{g}\}$;

• While ($P \neq \emptyset$)
  • choose $((\tilde{f}, f), (\tilde{g}, g)) \in P$;
  • $P := P \smallsetminus \{((\tilde{f}, f), (\tilde{g}, g))\}$;
  • $\tilde{h} := \mathrm{NF}(S(f, g)|S)$;
  • If ($\tilde{h} \neq 0$) then
    • Write $\tilde{h} = \sum_{(\tilde{g},g)} a_{(\tilde{g},g)} \cdot \tilde{g}$ with $a_{(\tilde{g},g)} \in \mathbf{k}[x, y]$;
      (this is possible by Definition 1.2.2(2)(3))
    • $h := \sum_{(\tilde{g},g)} a_{(\tilde{g},g)} \cdot g$;
    • $P := P \cup \{((\tilde{h}, h), (\tilde{f}, f)) \mid (\tilde{f}, f) \in S\}$;
    • $S := S \cup \{(\tilde{h}, h)\}$);
• Return S.

Remark.
- Notice that if we apply this algorithm to $G_2 = \{0\}$ then we obtain a set of couples $(\tilde{g}, 0)$. Thus in this situation it is equivalent to Standard.
- By construction, for any $(\tilde{g}, g)$ in the output S, $\tilde{g} \in \langle G_2 \rangle \iff g \in \langle G_2 \rangle$.
- Applying this algorithm to a basis G_J of J and a basis $G_{\mathcal{Q}}$ of $\mathcal{Q}$ we get as an output a set S of couples $(\tilde{g}, g)$. Then $\tilde{\mathcal{G}} = \{\tilde{g} | (\tilde{g}, g) \in S\}$ satisfies Proposition 3.2.2 and $\mathcal{G} = \{g | (\tilde{g}, g) \in S\}$ satisfies Corollary 3.2.3.
- Notice that this algorithm can be used in the general situation where we want a standard basis of the sum of two ideals I_1 and I_2 and such that each g in this basis can be decomposed as $g_1 + g_2$ with $g_i \in I_i$.

Returning to our initial question, we obtain a variant of PSBmod.

Algorithm 3.2.5 (PSBmod$'$).
Input: $G \subset \mathbf{k}[x, y]$: a finite set, $G_{\mathcal{Q}} \subset \mathbf{k}[y]$: a finite set.
Output: $\mathrm{PSBmod}'(G, G_{\mathcal{Q}}) = (\mathcal{G}, H)$ with $\mathcal{G}$: a pseudo standard basis of $\langle G \rangle$ modulo $\langle G_{\mathcal{Q}} \rangle$, $H \subset \mathbf{k}[y] \smallsetminus \langle G_{\mathcal{Q}} \rangle$: a finite set.
• Define a global order $\leq_0$ on $\mathbb{N}^m$;
• Form a block order $\leq := (\preceq, \leq_0)$;
• if $G \subset \langle G_{\mathcal{Q}} \rangle$ then return $(\emptyset, \emptyset)$;
• $S := \mathrm{ModifiedStandard}(G, G_{\mathcal{Q}}, \mathrm{NF})$ where NF is normal form for $\leq$;
• $\mathcal{G} := \{g \mid (\tilde{g}, g) \in S,\ g \notin \mathbf{k}[x, y]G_{\mathcal{Q}}\}$;
• $H := \emptyset$; for ($g \in \mathcal{G}$) do ($H := H \cup \{\mathrm{lc}_{\preceq}^{\bmod \langle G_{\mathcal{Q}} \rangle}(g)\}$);
• Return $(\mathcal{G}, H)$.

To end this part, let us note that if $\preceq$ is not global one may use a homogenization following Lazard (see Lemma 2.1.1).

4. Stratification with respect to a constant Exp

In 4.1, we shall prove Corollary 0.1.3 and Proposition 0.1.6(2).

In 4.2, 4.3 and 4.4, we propose different variants of an algorithm illustrating those results. In 4.2 the algorithm work for a general ring $\mathcal{C}$ while the algorithms in 4.3 and 4.4 work when $\mathcal{C}$ is of the form $\mathbf{k}[y]$.

4.1. **Proof of Cor. 0.1.3 and Prop. 0.1.6(2).** Let us recall that we start with an ideal $J \subset \mathcal{C}[x]$ and $\mathcal{C}$ is a noetherian integral domain.

We are going to describe a construction by induction on the step l. At each step l, we shall construct the following objects:

- A finite set $\mathfrak{W}_l$ of triples $(\mathcal{Q}, h, \mathcal{G})$ where $\mathcal{Q}$ is an ideal of $\mathcal{C}$, $h \in \mathcal{C}$ and $\mathcal{G}$ is finite set in J (the set $\mathfrak{W}_l$ may be empty),
- A finite set $\mathfrak{Q}_l$ of ideals $\mathcal{C}$ (this set may be empty),
- An ideal $\mathcal{I}_l$ of $\mathcal{C}$,

with the following properties:

(p1) $\mathrm{Spec}(\mathcal{C}) = (\bigcup_{(\mathcal{Q},h,\mathcal{G})\in\mathfrak{W}_l} V(\mathcal{Q}) \smallsetminus V(h)) \cup (\bigcup_{\mathcal{Q}\in\mathfrak{Q}_l} V(\mathcal{Q})) \cup V(\mathcal{I}_l)$,

(p2) For any $(\mathcal{Q}, h, \mathcal{G}) \in \mathfrak{W}_l$, and for any specialization $\sigma : \mathcal{C} \to \mathbf{K}$ such that $\sigma(\mathcal{Q}) = \{0\}$ and $\sigma(h) \neq 0$, $\sigma(\mathcal{G})$ is $\preceq$-standard basis of $\mathbf{K}[x]\sigma(J)$,

(p3) $J \subset \mathcal{C}[x] \cdot \mathcal{I}_l$ (i.e. J specializes to zero on $V(\mathcal{I}_l)$).

At step 0, we set $\mathfrak{W}_0 = \emptyset$ and $\mathfrak{Q}_0 = \{(0)\}$ and $\mathcal{I}_0 = \langle 1\rangle$.

Assume the objects of step l are constructed. If $\mathfrak{Q}_l = \emptyset$ then we stop the construction. Otherwise we define $\mathfrak{W}_{l+1}$, $\mathfrak{Q}_{l+1}$ and $\mathcal{I}_{l+1}$ as follows. Take $\mathcal{Q}$ in $\mathfrak{Q}_l$.

(A) If J is not included in $\mathcal{C}[x] \cdot \mathcal{Q}$.
Apply Theorem 0.1.1 to $\mathcal{Q}$. We obtain $\mathcal{G} \subset J$ and a finite number of $h_i \in \mathcal{C} \smallsetminus \mathcal{Q}$ $(i = 1, \ldots, r)$. We have $\mathcal{Q} \subsetneqq \mathcal{Q} + \langle h_i\rangle$.
Set $h = \prod_{i=}^{r} h_i$. Set $\mathfrak{Q}_{l+1} = (\mathfrak{Q}_l \smallsetminus \{\mathcal{Q}\}) \cup \{\mathcal{Q} + \langle h_i\rangle | i = 1, \ldots, r\}$.
Put $\mathfrak{W}_{l+1} = \mathfrak{W}_l \cup \{(\mathcal{Q}, h, \mathcal{G})\}$ and $\mathcal{I}_{l+1} = \mathcal{I}_l$.

(B) If J is included in $\mathcal{C}[x]\mathcal{Q}$.
Set $\mathfrak{Q}_{l+1} := \mathfrak{Q}_l \smallsetminus \{\mathcal{Q}\}$, $\mathfrak{W}_{l+1} = \mathfrak{W}_l$ and $\mathcal{I}_{l+1} := \mathcal{I}_l \cap \mathcal{Q}$.

It is clear that at each step l, properties (p1), (p2) and (p3) are satisfied. It is also clear that this construction is algorithmic if $\mathcal{C}$ is detachable and intersections are computable in $\mathcal{C}$. Moreover if $\sigma(J) \neq \{0\}$ for any specialization σ then $\mathcal{I}_l = \langle 1\rangle$ for all l (i.e. condition (B) is never satisfied). Thus, in order to prove Corollary 0.1.3 and Proposition 0.1.6(2), it is enough to prove that there exists l for which $\mathfrak{Q}_l$ is empty.

Assume by contradiction that for each l, there exists $\mathcal{Q} \in \mathfrak{Q}_l$ such that $J \not\subseteq \mathcal{C}[x]\mathcal{Q}$. This will imply the existence of an increasing sequence of ideals of $\mathcal{C}$ which contradicts the noetherianity of $\mathcal{C}$. Thus there exists l_0 such that for all $\mathcal{Q} \in \mathfrak{Q}_{l_0}$, $J \subseteq \mathcal{C}[x]\mathcal{Q}$. Thus for all steps $l_0, l_0 + 1, \ldots$, condition (B) is always satisfied. Thus after a finite number of steps, $\mathfrak{Q}_l$ becomes empty.

Remark 4.1.1.

(1) Applying this construction, we obtain a union of $\mathrm{Spec}(\mathcal{C})$ made of locally closed sets and on each of these sets Exp is constant. Comparing the values of Exp on the strata and forming unions of appropriate strata, we obtain the stratification by a constant Exp.

(2) Notice that given a triple $(\mathcal{Q}, h, \mathcal{G}) \in \mathfrak{W}_l$ we may have $V(\mathcal{Q}) \smallsetminus V(h) = \emptyset$ in $\mathrm{Spec}(\mathcal{C})$. Thus, such a triple is useless for the final stratification.

4.2. **Stratification algorithm 1.** This algorithm consists on a rewriting of the construction in 4.1.

Algorithm 4.2.1 (StratExp1)**.**

Input: $G \subset \mathcal{C}[x]$: a finite set.
Output: StratExp$(G) = (\{(\mathcal{Q}_1, h_1, \mathcal{G}_1), \ldots, (\mathcal{Q}_s, h_s, \mathcal{G}_s)\}, \mathcal{I})$;
where $\mathcal{Q}_i \subset \mathcal{C}$ is an ideal, $h_i \in \mathcal{C}$, $\mathcal{G}_i \subset \mathcal{C}[x] \cdot G$ is finite and $\mathcal{I} \subset \mathcal{C}$ is an ideal.

- $\mathfrak{W} := \emptyset$; $\mathfrak{Q} := \{(0)\}$; $\mathcal{I} := \mathcal{C} \cdot 1$;
- While $(\mathfrak{Q} \neq \emptyset)$
    - Choose $\mathcal{Q} \in \mathfrak{Q}$;
    - $\mathfrak{Q} := \mathfrak{Q} \smallsetminus \{\mathcal{Q}\}$;
    - $(\mathcal{G}, H) :=$ PSBmod$(G, \mathcal{Q})$;
    - if $((\mathcal{G}, H) \neq (\emptyset, \emptyset))$
      then • $h := \prod_{h' \in H} h'$;
      • $\mathfrak{Q} := \mathfrak{Q} \cup \bigcup_{h' \in H} \{\mathcal{Q} + \langle h' \rangle\}$;
      • $\mathfrak{W} := \mathfrak{W} \cup \{(\mathcal{Q}, h, \mathcal{G})\}$
      else • $\mathcal{I} := \mathcal{I} \cap \mathcal{Q}$;
- Return $(\mathfrak{W}, \mathcal{I})$.

Here, $(\mathcal{G}, H) \neq (\emptyset, \emptyset)$ corresponds to condition (A) in 4.1 and $(\mathcal{G}, H) = (\emptyset, \emptyset)$ corresponds to condition (B).

4.3. **Stratification algorithm 2.** Here we give a variant of the algorithm above in the case where $\mathcal{C} = \mathbf{k}[y] = \mathbf{k}[y_1, \ldots, y_m]$.

As we already noticed, in the output of StratExp1 we may have triples $(\mathcal{Q}, h, \mathcal{G})$ such that $V(\mathcal{Q}) \smallsetminus V(h)$ is empty. In the next variant we may replace the line
• $\mathfrak{W} := \mathfrak{W} \cup \{(\mathcal{Q}, h, \mathcal{G})\}$
of StratExp1 by
• if $(V(\mathcal{Q}) \nsubseteq V(h))$ then $\mathfrak{W} := \mathfrak{W} \cup \{(\mathcal{Q}, h, \mathcal{G})\}$
the question being how to check the "if" condition in an algorithmic way.

Let us analyse more deeply the construction in 4.1 and show how we may improve it. Let us take the notations of 4.1. We take $\mathcal{Q} \in \mathfrak{Q}_l$ such that we are under condition (A) (i.e. $J \nsubseteq \mathcal{C}[x]\mathcal{Q}$). Applying Theorem 0.1.1, we obtain $\mathcal{G} \subset J$ and $h_1, \ldots, h_r \in \mathcal{C} \smallsetminus \mathcal{Q}$. We have:

$$V(\mathcal{Q}) = (V(\mathcal{Q}) \smallsetminus V(h)) \bigsqcup \left(\bigcup_{i=1}^{r} V(\mathcal{Q} + \langle h_i \rangle) \right).$$

The next step consists in adding the triple $(\mathcal{Q}, h, \mathcal{G})$ to $\mathfrak{W}_l$ and to add the ideals $\mathcal{Q} + \langle h_i \rangle$ to $\mathfrak{Q}_l$.

Although $\mathcal{Q} \subsetneq \mathcal{Q} + \langle h_i \rangle$, we may have $V(\mathcal{Q}) = V(\mathcal{Q} + \langle h_i \rangle)$. Thus in step $l+1$, it would be useless to apply the construction to $\mathcal{Q} + \langle h_i \rangle$ if $V(\mathcal{Q}) = V(\mathcal{Q}) + \langle h_i \rangle$ i.e. $V(\mathcal{Q}) \subseteq V(h_i)$. Therefore, we would like to replace the line
• $\mathfrak{Q} := \mathfrak{Q} \cup \bigcup_{h' \in H} \{\mathcal{Q} + \langle h' \rangle\}$
of StratExp1 by
• $\mathfrak{Q} := \mathfrak{Q} \cup \bigcup_{h' \in H, V(\mathcal{Q}) \smallsetminus V(h') \neq \emptyset} \{\mathcal{Q} + \langle h' \rangle\}$.

Now from an algorithmic point of view how can we check if a given h is such that $V(\mathcal{Q}) \smallsetminus V(h) \neq \emptyset$? The answer is in the following version of Hilbert's Nullstellensatz theorem.

Lemma 4.3.1. *Let* $\mathbf{k}$ *be any field. Let* $\mathcal{Q} \subset \mathbf{k}[y] = \mathbf{k}[y_1, \ldots, y_m]$ *be an ideal. For any* $h \in \mathbf{k}[y]$*, we have:*

$$h \in \sqrt{\mathcal{Q}} \iff V(\mathcal{Q}) \smallsetminus V(h) \text{ is empty in } \operatorname{Spec}(\mathbf{k}[y]).$$

Proof. We have to prove that $h \in \sqrt{\mathcal{Q}}$ if and only if $V(\mathcal{Q}) \subset V(h)$. The left-right implication is trivial. Let us assume that $V(\mathcal{Q}) \subset V(h)$.

Let $\mathbf{K}$ be any algebraically closed field containing $\mathbf{k}$. Firstly, we have $(\mathbf{K}[y]\mathcal{Q}) \cap \mathbf{k}[y] = \mathcal{Q}$. Indeed, by Remark 1.2.6, any Gröbner basis of $\mathcal{Q}$ (with respect to a global order) is a Gröbner basis of $\mathbf{K}[y]\mathcal{Q}$.

Now, given a prime ideal $\mathcal{P} \subset \mathbf{K}[y]$, the set $\mathbf{k}[y] \cap \mathcal{P}$ is a prime ideal of $\mathbf{k}[y]$. If $\mathcal{P}$ contains $\mathbf{K}[y]\mathcal{Q}$ then $\mathcal{P} \cap \mathbf{k}[y]$ contains $(\mathbf{K}[y]\mathcal{Q}) \cap \mathbf{k}[y] = \mathcal{Q}$. Thus the hypothesis implies that $h \in \mathcal{P}$. Therefore we have: $\{y \in \mathbf{K}^m | y \in V_{\mathbf{K}}(\mathcal{Q}) \smallsetminus V_{\mathbf{K}}(h)\}$ is empty. Here $V_{\mathbf{K}}$ stands for the zero set of. By the classical Hilbert's Nullstellensatz theorem, $h^i \in \mathbf{K}[y]\mathcal{Q}$ for some integer i. Finally we obtain: $h^i \in (\mathbf{K}[y]\mathcal{Q}) \cap \mathbf{k}[y] = \mathcal{Q}$. $\square$

Notice that in $\mathbf{k}[y]$, checking whether $h \in \sqrt{\mathcal{Q}}$ does not require the computation of a Gröbner basis of $\sqrt{\mathcal{Q}}$, see e.g. [GrPf02b, §1.8.6].

Gathering the previous remarks we obtain the next algorithm.

Algorithm 4.3.2 (StratExp2)**.**
Input: $G \subset \mathbf{k}[y][x]$: a finite set.
Output: $\operatorname{StratExp}(G) = (\{(\mathcal{Q}_1, h_1, \mathcal{G}_1), \ldots, (\mathcal{Q}_s, h_s, \mathcal{G}_s)\}, \mathcal{I})$,
where $\mathcal{Q}_i \subset \mathbf{k}[y]$ is a finitely generated ideal, $h_i \in \mathbf{k}[y]$, $\mathcal{G}_i \subset \mathbf{k}[y][x] \cdot G$ is finite and $\mathcal{I} \subset \mathbf{k}[y]$ is an ideal.

- $\mathfrak{W} := \emptyset$; $\mathfrak{Q} := \{(0)\}$; $\mathcal{I} := \mathbf{k}[y] \cdot 1$;
- While $(\mathfrak{Q} \neq \emptyset)$
    - Choose $\mathcal{Q} \in \mathfrak{Q}$; (let $G_{\mathcal{Q}}$ denote a finite basis)
    - $\mathfrak{Q} := \mathfrak{Q} \smallsetminus \{\mathcal{Q}\}$;
    - $(\mathcal{G}, H) := \operatorname{PSBmod}(G, \mathcal{Q})$ or $(\mathcal{G}, H) := \operatorname{PSBmod}'(G, G_{\mathcal{Q}})$;
    - if $((\mathcal{G}, H) \neq (\emptyset, \emptyset))$
        then • $h := \prod_{h' \in H} h'$;
        • $H := \{h' \in H \mid h' \notin \sqrt{Q}\}$;
        • $\mathfrak{Q} := \mathfrak{Q} \cup \bigcup_{h' \in H} \{\mathcal{Q} + \langle h' \rangle\}$;
        • if $(h \notin \sqrt{\mathcal{Q}})$ then $\mathfrak{W} := \mathfrak{W} \cup \{(\mathcal{Q}, h, \mathcal{G})\}$
        else • $\mathcal{I} := \mathcal{I} \cap \mathcal{Q}$;
- Return $(\mathfrak{W}, \mathcal{I})$.

4.4. **Stratification algorithm 3.** Here we give a usual stratification algorithm for $\mathcal{C} = \mathbf{k}[y]$. It uses primary (or prime) decomposition. In the construction process, all the output tiples $(\mathcal{Q}, h, \mathcal{G})$ are such that $\mathcal{Q}$ is prime. Since h is a product of $h' \in \mathbf{k}[y] \smallsetminus \mathcal{Q}$, we shall have $h \notin \mathcal{Q}$.

We shall give the algorithm without proofs for correctness and termination since it is well-known.

Algorithm 4.4.1 (StratExp3)**.**
Input: $G \subset \mathbf{k}[y][x]$: a finite set.
Output: $\operatorname{StratExp}(G) = (\{(\mathcal{Q}_1, h_1, \mathcal{G}_1), \ldots, (\mathcal{Q}_s, h_s, \mathcal{G}_s)\}, \mathcal{I})$;
where $\mathcal{Q}_i \subset \mathbf{k}[y]$ is a finitely generated prime ideal, $h_i \in \mathbf{k}[y] \smallsetminus \mathcal{Q}$, $\mathcal{G}_i \subset \mathbf{k}[y][x] \cdot G$ is finite and $\mathcal{I} \subset \mathbf{k}[y]$ is an ideal.

- $\mathfrak{W} := \emptyset$; $\mathfrak{Q} := \{(0)\}$; $\mathcal{I} := \mathbf{k}[y] \cdot 1$;
- While $(\mathfrak{Q} \neq \emptyset)$
  - Choose $\mathcal{Q} \in \mathfrak{Q}$; (let $G_{\mathcal{Q}}$ denote a finite basis)
  - $\mathfrak{Q} := \mathfrak{Q} \smallsetminus \{\mathcal{Q}\}$;
  - $(\mathcal{G}, H) := \mathrm{PSBmod}(G, \mathcal{Q})$ or $(\mathcal{G}, H) := \mathrm{PSBmod}'(G, G_{\mathcal{Q}})$;
  - if $((\mathcal{G}, H) \neq (\emptyset, \emptyset))$

    then • $h := \prod_{h' \in H} h'$;

    • Compute prime ideals $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ of $\mathbf{k}[y]$ such that $V(\mathcal{Q} + \langle h \rangle) = V(\mathcal{Q}_1) \cup \cdots \cup V(\mathcal{Q}_r)$;

    • $\mathfrak{Q} := \mathfrak{Q} \cup \{\mathcal{Q}_1, \ldots, \mathcal{Q}_r\}$;

    • $\mathfrak{W} := \mathfrak{W} \cup \{(\mathcal{Q}, h, \mathcal{G})\}$

    else • $\mathcal{I} := \mathcal{I} \cap \mathcal{Q}$;
- Return $(\mathfrak{W}, \mathcal{I})$.

5. Stratification by the local Hilbert-Samuel function

Proof of Corollary 0.2.1. Recall that we start with a finitely generated ideal $I \subset \mathbf{k}[x] := \mathbf{k}[x_1, \ldots, x_n]$ and a field inclusion $\mathbf{k} \subset \mathbf{K}$. Let $f_1, \ldots, f_q$ be generators of I. Consider the following ideal $J = \sum_{l=1}^{q} \mathbf{k}[x, y] \cdot f_l(x + y)$ where y stands for $(y_1, \ldots, y_n)$. Take a valuation-compatible order $\preceq$ on the x^{α}'s. Apply Corollary 0.1.3 to $J \subset \mathbf{k}[y][x]$. We obtain $\mathcal{G}_1, \ldots, \mathcal{G}_r \in J$ and

$$\mathrm{Spec}(\mathbf{k}[y]) = (\bigcup_{k=1}^{r} W_k) \cup V(\mathcal{I}))$$

where W_k are constructible sets of $\mathrm{Spec}(\mathbf{k}[y])$ and $\mathcal{I} \subset \mathbf{k}[y]$ is an ideal. We have that for any specialization σ of $\mathbf{k}[y]$, if $\sigma(\mathcal{I}) = \{0\}$ then $\sigma(J) = \{0\}$. Denote by $\overline{\mathbf{k}}$ the algebraic closure of $\mathbf{k}$ and consider the specializations $\sigma_{y_0} = (\mathbf{k}[y] \to \overline{\mathbf{k}}, P(y) \mapsto P(y_0))$ where $y_0 \in \overline{\mathbf{k}}^n$. If the zeroset $V_{\overline{\mathbf{k}}}(\mathcal{I}) \subset \overline{\mathbf{k}}^n$ is not empty then for any $y_0 \in V_{\overline{\mathbf{k}}}(\mathcal{I})$ we have $\overline{\mathbf{k}}[x] \cdot J_{|y=y_0} = \{0\}$ but this is impossible since we implictely supose $I \neq \{0\}$. Thus $V_{\overline{\mathbf{k}}}(\mathcal{I})$ is empty, therefore $1 \in \overline{\mathbf{k}}[y]\mathcal{I}$ i.e. $1 \in \mathcal{I}$ and the affine scheme $V(\mathcal{I}) \subset \mathrm{Spec}(\mathbf{k}[y])$ is empty, therefore $\mathrm{Spec}(\mathbf{k}[y]) = (\bigcup_{k=1}^{r} W_k)$.

Now for any specialization $\sigma : \mathbf{k}[y] \to \mathbf{K}$ such that $\sigma(W_k) = \{0\}$, $\sigma(\mathcal{G}_k)$ is a $\preceq$-standard basis of $\mathbf{K}[x]\sigma(J)$ and $\mathrm{Exp}_{\preceq}(\mathbf{K}[x]\sigma(J))$ does not depend on σ. We consider specializations of the form $\sigma_{x_0} = (\mathbf{k}[y] \to \mathbf{K}, P(y) \mapsto P(x_0))$ where $x_0 \in \mathbf{K}^m$ and use Lemmas 1.3.2 and 1.3.1(2) to conclude. □

Proof of Corollary 0.2.2. We sketch the proof since it is similar to the previous one. Recall that we have an ideal $I \subset \mathbb{Z}[a, x]$ given by polynomials $f_j = f_j(a, x)$. Introduce a new set y of indeterminates $y_1, \ldots, y_n$ and consider the ideal $J = \sum_j \mathbb{Z}[a, y][x] \cdot f_j(a, x + y) \subset \mathbb{Z}[a, y][x]$. We may apply Corollary 0.1.3 and use the same arguments as above. □

6. Examples

Here we shall give some examples of the computation of a stratification by the local Hilbert-Samuel function. These examples (except example 1 treated by hand) were computed with a program (available on the author's webpage) written using Risa/Asir computer algebra system [No].

In Examples 2 to 5, the output is presented as follows:
$[[[\alpha_1, \alpha_2, \ldots], [q_1(x), q_2(x), \ldots], [h_1(x), h_2(x), \ldots]], \ldots]$,
where $\alpha_i \in \mathbb{N}^n$, $q_i, h_i \in \mathbb{C}[x]$.

This means that for $x_0 \in V(\langle q_1, q_2, \ldots\rangle) \setminus V(h_1 \cdot h_2 \cdots)$, the local Hilbert-Samuel function at x_0 is equal to that of the monomial ideal $\langle x^{\alpha_1}, x^{\alpha_2}, \ldots\rangle$.

6.1. **Example 1.** Set $f = {x_1}^2 + {x_2}^3$ and $I = \mathbb{C}[x_1, x_2]f$.

In this case we shall only use the fact that the Hilbert-Samuel function associated with f at $x = x_0$ is equal to that associated with $f(x + x_0)$ at $x = 0$.

Let us write $f(x + y)$ as a Taylor series:

$$f(x+y) = (y_1^2 + y_2^3) + (2y_1x_1 + 3y_2^2x_2) + (x_1^2 + 3y_2x_2^2) + (x_2^3).$$

This expansion respects the valuation in x. Let us consider a valuation-compatible order on the x-monomials. For $\preceq$, the leading term of $f(x + y)$ is 1 and the leading coefficient is $v = y_1^2 + y_2^3$. On $\mathbb{C}^2 \setminus \{v = 0\}$, the Hilbert-Samuel function is zero. Now let us work on the space $V := \{v = 0\}$. Here, working modulo v, we can write

$$f(x+y) \equiv (2y_1x_1 + 3y_2^2x_2) + (x_1^2 + 3y_2x_2^2) + (x_2^3).$$

Again we fix a monomial order on x as above. Notice that we have some freedom: we can choose $\preceq$ in order that the leading term is x_1 or x_2 with the corresponding leading coefficients $2y_1$ or $3y_2^2$. Let us choose the leading monomial as $2y_1 \cdot x_1$. We obtain that on $V \setminus \{(0, 0)\}$, the Hilbert-Samuel function equals that of $\mathbb{C}[x_1, x_2]/\langle x_1\rangle$. Finally, it remains $\{(0, 0)\}$ (i.e. we work modulo $\langle y_1, y_2\rangle$) on which

$$f(x+y) \equiv x_1^2 + x_2^3.$$

Finally, we get the stratification

$$\mathbb{C}^2 = (\mathbb{C}^2 \setminus V) \cup (V \setminus \{(0,0)\}) \cup \{(0,0)\}$$

such that one each statum the local Hilbert-Samuel function is constant and equal to $\mathbb{N} \ni r \to 0$, $\mathrm{HSF}_{\mathbb{C}[x_1,x_2]/\langle x_1\rangle}$, and $\mathrm{HSF}_{\mathbb{C}[x_1,x_2]/\langle x_1^2\rangle}$ respectively.

6.2. **Example 2.** The same example : $I = \mathbb{C}[x_1, x_2]\cdot(x_1^2+x_2^3)$. Our program outputs:

```
[[[(1)*<<0,0>>],[0],[x1^2+x2^3]],
[[(1)*<<0,1>>,(1)*<<0,1>>],[x1^2+x2^3],[x2,x1]],
[[(1)*<<2,0>>],[x2,x1],[1]]]
```

We have the following interpretation: On any point of $V(0) \setminus V(x_1^2 + x_2^3)$, the local Hilbert-Samuel function associated with I is the same as that of $\mathbb{C}[x_1, x_2]/\langle x_1^0x_2^0\rangle = \mathbb{C}[x_1, x_2]/\langle 1\rangle$. On any point of $V(x_1^2 + x_2^3) \setminus V(x_2 \cdot x_1)$, we get the Hilbert-Samuel function of $\mathbb{C}[x_1, x_2]/\langle x_2\rangle$. On any point of $V(\langle x_2, x_1\rangle) \setminus V(1)$ (i.e. at $x = (0, 0)$), we get the Hilbert-Samuel function of $\mathbb{C}[x_1, x_2]/\langle x_1^2\rangle$. We recover the results of Example 1.

6.3. **Example 3.** Here, we set $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3 x_1^2 x_2$ and $I = \mathbb{C}[x_1, x_2, x_3] \cdot f$. The output is :

```
[[[(1)*<<0,0,0>>],[0],[x1^4+x3*x2*x1^2+x2^4]],
[[(1)*<<0,0,1>>,(1)*<<0,0,1>>],[x1^4+x3*x2*x1^2+x2^4],[x1,x2*x1]],
[[(1)*<<2,1,0>>],[x2,x1],[x3]],
[[(1)*<<0,4,0>>],[x3,x2,x1],[1]]]
```

By line 2, we get: On $V(f) \setminus V(x_1 x_2)$, the local Hilbert-Samuel function is equal to that of $\mathbb{C}[x_1, x_2, x_3]/\langle x_3 \rangle$.
By line 3, we get: On $V(\langle x_1, x_2 \rangle) \setminus V(x_3)$, we have the same Hilbert-Samuel function as $\mathbb{C}[x_1, x_2, x_3]/\langle x_1^2 x_2 \rangle$.
By line 3, we get: at $x = (0, 0, 0)$, the Hilbert-Samuel function is the same as that of $\mathbb{C}[x_1, x_2, x_3]/\langle x_2^4 \rangle$.

6.4. **Example 4.** Set $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3 x_1 x_2$ and $I = \mathbb{C}[x_1, x_2, x_3] \cdot f$. The program outputs:

```
[[[(1)*<<0,0,0>>],[0],[x1^4+x3*x2*x1+x2^4]],
[[(1)*<<0,0,1>>,(1)*<<0,0,1>>],[x1^4+x3*x2*x1+x2^4],[x1,x2*x1]],
[[(1)*<<1,1,0>>],[x2,x1],[x3]],
[[(1)*<<1,1,1>>],[x3,x2,x1],[1]]]
```

By line 2, we get the Hilbert-Samuel function of $\mathbb{C}[x_1, x_2, x_3]/\langle x_3 \rangle$ on $V(f) \setminus V(x_1 x_2)$. By line 3, we get the Hilbert-Samuel function of $\mathbb{C}[x_1, x_2, x_3]/\langle x_1 x_2 \rangle$ on $V(\langle x_1, x_2 \rangle) \setminus V(x_3)$. Finally at $x = (0, 0, 0)$ we get the Hilbert-Samuel function of $\mathbb{C}[x_1, x_2, x_3]/\langle x_1 x_2 x_3 \rangle$.

6.5. **Example 5.** Here, we set $f_1 = x_1 - x_2$ and $f_2 = x_1(x_2^2 + x_3^3)$ and $I = \mathbb{C}[x_1, x_2, x_3]\{f_1, f_2\}$. We get the following output (we numbered the lines):

```
(1)  [[[(1)*<<0,0,0>>,(1)*<<0,0,0>>],[0],[x1^3+x3^3*x1,-x1+x2]],
(2)  [[(1)*<<0,0,0>>,(1)*<<0,1,0>>],[-x1+x2],[x1^3+x3^3*x1,1]],
(3)  [[(1)*<<0,0,1>>,(1)*<<0,0,1>>,(1)*<<0,1,0>>],
     [-x1+x2,x2^2+x3^3],[x3*x1,x1,1]],
(4)  [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]],
(5)  [[(1)*<<0,1,0>>,(1)*<<1,0,0>>],[x2,x1],[1,x3]],
(6)  [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]],
(7)  [[(1)*<<0,0,0>>,(1)*<<0,0,1>>,(1)*<<0,0,1>>],
     [x1^2+x3^3],[-x1+x2,x3*x1,x1]],
(8)  [[(1)*<<0,0,1>>,(1)*<<0,0,1>>,(1)*<<0,1,0>>],
     [-x1+x2,x2^2+x3^3],[x3*x1,x1,1]],
(9)  [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]],
(10) [[(1)*<<0,0,0>>,(1)*<<3,0,0>>],[x3,x1],[x2,1]],
(11) [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]],
(12) [[(1)*<<0,0,0>>,(1)*<<1,0,0>>],[x1],[x2,x3]],
(13) [[(1)*<<0,1,0>>,(1)*<<1,0,0>>],[x2,x1],[1,x3]],
(14) [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]],
(15) [[(1)*<<0,0,0>>,(1)*<<3,0,0>>],[x3,x1],[x2,1]],
(16) [[(1)*<<0,1,0>>,(1)*<<3,0,0>>],[x3,x2,x1],[1,1]]].
```

Some lines appear several times (e.g. lines 4, 6, 9, 11, 14 and 16 are equal since they are the termination leaf of several branches of the tree). In this

result, line 2 (for example) means that on $V(f_1) \setminus V(f_2)$ the Hilbert-Samuel function is given by that of $\mathbb{C}[x_1, x_2, x_3]/\langle 1, x_2\rangle = \mathbb{C}[x_1, x_2, x_3]/\langle 1\rangle$. Line 5 means that on $V(\langle x_1, x_2\rangle) \setminus \{0\}$ the Hilbert-Samuel function is given by that $\mathbb{C}[x_1, x_2, x_3]/\langle x_1, x_2\rangle$.

References

[As04] M. Aschenbrenner, Ideal membership in polynomial rings over the integers. J. Amer. Math. Soc. 17 (2004), no. 2, 407–441

[As05] M. Aschenbrenner, Reduction mod p of standard bases. Comm. Algebra 33 (2005), no. 5, 1635–1661.

[AsLe09] M. Aschenbrenner, A. Leykin, Degree bounds for Gröbner bases in algebras of solvable type. J. Pure Appl. Algebra 213 (2009), no. 8, 1578–1605.

[As94] A. Assi, On flatness of generic projections. J. Symbolic Comput. 18 (1994), no. 5, 447–462.

[Ay83] C. W. Ayoub, On constructing bases for ideals in polynomial rings over the integers. J. Number Theory 17 (1983), no. 2, 204–225.

[Ba06] R. Bahloul, Polynôme de Bernstein-Sato générique local. J. Math. Soc. Japan 58 (2006), no. 2, 595–616.

[CLO92] D. Cox, J. Little, D. O'Shea, Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[Dub90] T. W. Dubé, The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. 19 (1990), no. 4, 750–775.

[GaMi94] G. Gallo, B. Mishra, A solution to Kronecker's problem. Appl. Algebra in Engrg. Comm. Comput. 5 (1994), no. 6, 343–370.

[GTZ05] L. Gonzalez-Vega, C. Traverso, A. Zanoni, Hilbert stratification and parametric Gröbner bases. Computer algebra in scientific computing, 220–235, Lecture Notes in Comput. Sci., 3718, Springer, Berlin, 2005.

[Gi89] P. Gianni, Properties of Gröbner bases under specializations. EUROCAL'87 (Leipzig, 1987), 293–297, Lecture Notes in Comput. Sci. 378, Springer, Berlin, 1989.

[GrPf02a] G.-M. Greuel, G. Pfister, Computer algebra and finite groups. Mathematical software (Beijing, 2002), 4–14, World Sci. Publishing, River Edge, NJ, 2002.

[GrPf02b] G.-M. Greuel, G. Pfister, A Singular introduction to commutative algebra. Springer-Verlag, Berlin, 2002.

[Ka97] M. Kalkbrener, On the stability of Gröbner bases under specializations. J. Symbolic Comput. 24 (1997), no. 1, 51–58.

[La83] D. Lazard, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. EUROCAL'83, 146–156, Lecture Notes in Comput. Sci. 162, Springer, Berlin, 1983.

[LePh89] M. Lejeune-Jalabert, A. Philippe, Un algorithme de calcul de changements de coordonnées génériques. C. R. Acad. Sci. Paris Sér. I Math. 309 (1989), no. 13, 803–806.

[Mo02] A. Montes, A new algorithm for discussing Gröbner bases with parameter. J. Symbolic Comput. 33 (2002), no. 2, 183–208.

[Mo82] F. Mora, An algorithm to compute the equations of tangent cones. Computer algebra (Marseille, 1982), pp. 158–165, Lecture Notes in Comput. Sci., 144, Springer, Berlin-New York, 1982.

[No] Noro et al., Risa/Asir: an open source general computer algebra system, Developed by Fujitsu Labs LTD, Kobe Distribution by Noro et al., see http://www.math.kobe-u.ac.jp/Asir/index.html.

[SaSu03] A. Suzuki, Y. Sato, An alternative approach to comprehensive Gröbner bases. J. Symbolic Comput. 36 (2003), no. 3-4, 649–667.

[We92] V. Weispfenning, Comprehensive Gröbner bases. J. Symbolic Comput. 14 (1992), no. 1, 1–29.

[We03] V. Weispfenning, Canonical comprehensive Gröbner bases. J. Symbolic Comput. 36 (2003), no. 3-4, 669–683.

Institut Camille Jordan, Université Claude Bernard - Lyon 1, 43 Boulevard du 11 novembre 1918, 69622 Villeurbanne, France

E-mail address: bahloul@math.univ-lyon1.fr